

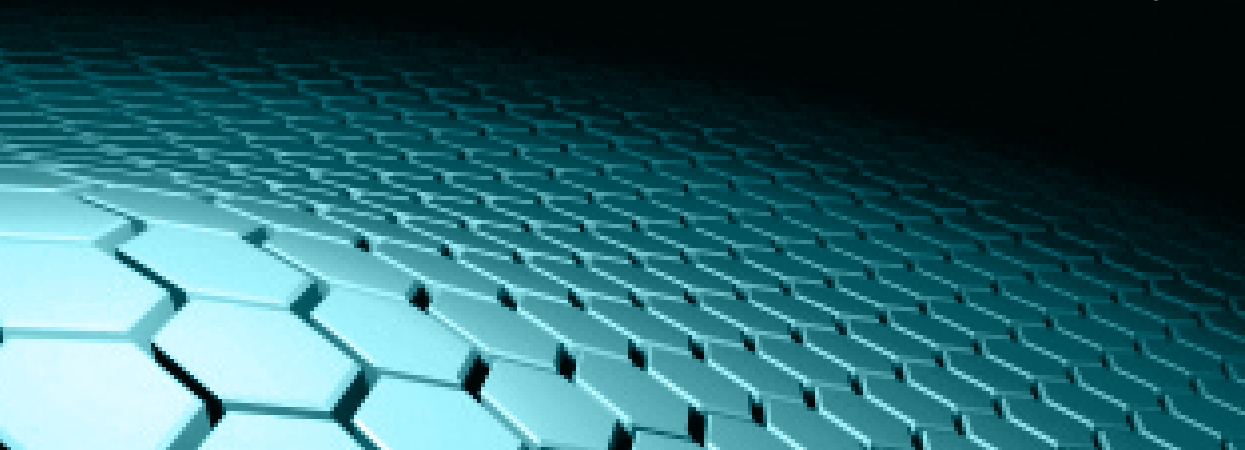


Australian Government
Department of Defence

Review of Social Media and Defence

Report by George Patterson Y&R

Reviews into aspects of Defence and
Australian Defence Force Culture
2011



REVIEW OF SOCIAL MEDIA AND DEFENCE

©Commonwealth of Australia 2011

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Department of Defence.

All Defence information, whether classified or not, is protected from unauthorised disclosure under the *Crimes Act 1914*. Defence information may only be released in accordance with the Defence Protective Security Manual and/or Defence Instruction (General) OPS 13-4—*Release of Classified Defence Information to Other Countries*, as appropriate.

Author: George Patterson Y&R

Sponsor: Vice Chief of Defence Force

Contact: First Assistant Secretary, Ministerial and Executive Coordination and Communication

ISBN 978-0-642-29750-1

CONTENTS

FOREWORD	VII
EXECUTIVE SUMMARY	IX
Social media – a revolution for all of society	ix
Defence culture and social media	x
The Defence brands	xii
Social media policy and guidelines	xvii
Education and social media	xviii
Operations and social media	xx
RECOMMENDATIONS	XXIII
Recommendation 1 (Unified strategy)	xxiii
Recommendation 2 (Policy)	xxiv
Recommendation 3 (Education)	xxiv
Recommendation 4 (Resourcing)	xxv
Recommendation 5 (Channel/content plan)	xxv
Recommendation 6 (Crisis management)	xxv
Recommendation 7 (Brand)	xxvi
OVERVIEW	XXVII
TERMS OF REFERENCE	XXIX
CONDUCT OF THE REVIEW	XXXIII
RISKS AND LIMITATIONS	XXXV
STRUCTURE OF THE REVIEW	XXXVII
1.1 WHAT IS CULTURE?	3
1.2 What are social media?	5
2.1 Trends	10
2.2 Legal obligations	10
2.1 TRENDS	12
2.1.1 Trend: Australians among the heaviest users	12
2.1.2 Trend: Social media during natural disasters	14
2.1.3 Trend: Conversation drives interaction	16
2.1.4 Trend: Emerging platforms	17
2.1.5 Trend: Facebook dominates	18
2.1.6 Trend: Social media are mobile	22
2.1.7 Trend: Social media integrate with technology	24
2.1.8 Trend: Privacy is the new battleground	26
2.1.9 Trend: Social media alter news reporting	28

2.2 LEGAL OBLIGATIONS	30
Overview	30
Introduction	32
Social media engagement in context	33
User-Generated content	34
Regulation of Social Content	35
Laws Influencing and Restricting Defence Engagement in Social Media	37
The rules of proprietary space	63
Social media engagement principles	64
Social media policies	68
CLOSING OBSERVATIONS	72
3.1 MANAGEMENT	77
3.1.1 International best practice	77
3.1.2 Defence practices and attitudes	94
3.1.3 Discussion	119
3.2 MORALE	121
3.2.1 International best practice	121
3.2.2 Defence practices and attitudes	124
3.2.3 Discussion	132
3.3 MARKETING	133
3.3.1 International best practice	133
3.3.2 Defence practices and procedures	146
3.3.3 Discussion	156
4.1 INTRODUCTION	163
4.1.1 Strategy management	166
4.1.2 Campaign strategy	167
4.1.3 Goals and objectives	168
4.1.4 Australian Defence Force mission statements	169
4.1.5 Moderation	171
4.1.6 Monitoring	172
4.1.7 Branding	173
4.1.8 Crisis management	173
4.1.9 Channel strategy	174
4.2 BRANDING STRATEGY	175
4.2.1 Brand health	175
4.2.2 Employer brand	177
4.2.3 Channel ownership	178
4.2.4 Brand assets	179

4.2.5 Recruitment branding	180
4.2.6 'Test and learn'	180
4.2.7 Department of Defence – a different brand?	180
4.2.8 Point of failure – reliance on individuals	181
4.2.9 Content strategy	181
4.3 POLICY STRATEGY FRAMEWORK	183
4.3.1 Policy components	183
4.3.2 Policy for personnel who manage 'official' social media	186
4.3.3 Social media engagement principles	186
4.3.4 Policy development and implementation	188
4.3.5 Role of social media in Defence	189
4.3.6 Current policy on social media	189
4.3.7 Alignment with other policies	190
4.3.8 Standard operating procedures for personnel	190
4.3.9 Education	191
4.4 CRISIS MANAGEMENT STRATEGY	193
4.4.1 Crisis identification	196
4.4.2 Tips for communications staff in responding to a social media crisis	196
4.4.3 Emergency response monitoring	197
4.4.4 The 'knowledge void'	197
4.4.5 Crisis exit strategy	198
ANNEX 1 QUALITATIVE AND QUANTITATIVE RESEARCH	A1-3
ANNEX 2 PUBLIC PERCEPTIONS	A2-3
Australian Defence Force – Public perceptions	A2-4
Australian Army – Public perceptions	A2-7
Royal Australian Navy – Public perceptions	A2-10
Royal Australian Air Force – Public perceptions	A2-13
Public perceptions – Discussion	A2-16
ANNEX 3: OFFICIAL AND UNOFFICIAL SOCIAL MEDIA CHANNELS	A3-1
2.3.2 Royal Australian Navy	A3-7
2.3.3 Australian Army	A3-14
2.3.4 Royal Australian Air Force	A3-20
GLOSSARY AND REFERENCES	G-1

FOREWORD

For two decades now, globalisation has been sweeping the world, bringing people, business and government with it, in an unstoppable shrinking of the Earth and its boundaries. For thousands of years, people from across the globe travelled, traded and intermingled. What is different now is that with the advent of the World Wide Web people have become even closer. Communications and connections between people have been truly globalised in a way that our ancestors could never have imagined. When people communicate today, distance is no barrier. This brave new world of communications has encompassed the modern tools of what are now called *social media*. Social media are all around us, in our homes, our classrooms and our workplaces and as a support, entertainment and communication tool for our defence force personnel while they are at home or on deployment. As all organisations need to adapt to the ever-changing online environment, so too will Defence need to meet the challenges of using social media, both now and in the future.

This review examines the challenges for Defence of social media as they exist now and how they might evolve in the future. It examines the perceptions and attitudes of Defence personnel and the Australian community at large. It assesses international best practice, so that we might learn from others and so that Australia can be at the forefront of social media use by defence organisations. Finally, it suggests a plan to help support Defence to meet its obligations and make the best use of social media and the opportunities they can offer.

This review would not have been possible without the support of Defence. The organisation has been generous and open, both with its time and in allowing access to information and personnel. Without the support of those individuals in Defence who have acted as reactors in surveys, questionnaires and feedback, this review could not have occurred. The armed forces of the United States of America, the United Kingdom, Canada and New Zealand have been similarly generous with information about their policies and experience with social media.

I cannot complete this foreword without thanking the staff of the George Patterson Y&R organisation, who have worked tirelessly to produce this document. This review could not have been produced without their relentless hours of work, their commitment and their loyalty to the team and this review.

Rob Hudson

National Digital Director
George Patterson Y&R

EXECUTIVE SUMMARY

Social media – a revolution for all of society

A revolution is occurring in the way people communicate, driven by the use of social media. Although the revolution has been coming for some time, it has taken many in business, government and the general populace by surprise. The surprise has not just been about the widespread use of the new media, but about how they are changing the way business is conducted and how people communicate with business and government. Social media channels provide opportunities for all, but like all media they can have both positive and negative outcomes for individuals and organisations.

Defence is in a similar position to other organisations that are coming to grips with the social media. The Defence experience examined by the review team generally reflects that of the rest of Australian society. There is no evidence of systemic abuse by Defence personnel in their official or unofficial use of social media, which would bring the brand into disrepute or threaten operational security.

There is a view in the community that it is younger people who welcome social media and have been captured by it. Through research, this review concluded that Defence personnel across all age groups hold a continuum of views, from acceptance of social media and their likely benefits for Defence work to a rejection of them. Many accept that social media are here to stay and are willing to engage, but to varying degrees.

Those who are yet to welcome social media into their lives may be reflecting the traditions of security and confidentiality within Defence. In some ways, those traditions are contradictory to the philosophies of social media, where openness and transparency often take a higher priority.

There is nothing unusual about the continuum of opinions in Defence, as it reflects the variety of views about social media in the wider Australian society. However, Defence personnel in Australia have a peculiar position in society because of the work they do and because of the Australian community's high regard for them.

The review team was conscious of the terms of reference for this report, but also understood that its work might provide a snapshot of social media within Defence and a blueprint for future developments.

The team prepared this review from a composite of research, observations and findings in the form of a synthesis report. It conducted general research, including by examining and assessing international social media policies, strategies and protocols from material produced by other armed forces. It also conducted quantitative and qualitative research to gauge attitudes, perceptions and views about social media in the general community and within Defence.

The need to examine and review extensive material and conduct research in the time allowed for this review meant that the review team could not access every possibly relevant source. However, some themes outlined in this report are so strong that they are likely to truly reflect current social media trends, uses, attitudes and needs in Defence. This review provides conclusions and proposals, which will stimulate discussion within Defence and among its stakeholders about social media and their role in Defence's future.

Defence culture and social media

The convergence of conversations

The wide variety of opinions held by Defence personnel about the organisation's use of social media reveals some polarisation and inconsistencies. Recent events have heightened sensitivity about social media use and shown that some individuals do not understand the potential breadth and depth of communication in that space.

The division of opinions within Defence has manifested itself most prominently in a debate about balancing security and transparency. Others see this simply as a jurisdictional issue – operations versus corporate communication. This review has noted a division that spans organisation, rank, level, role, age and gender. No demographic supports either argument consistently.

One of the themes identified in many qualitative interviews is a high level of risk aversion about engaging in social media, which extends to communicating with the media in general. It is undeniably true that the subjects of social media and security are inextricably linked in the Defence culture, partly because the security aspect of these 'new' media was emphasised by those who spoke first and loudest on the subject within the organisation. The culture and approach of Defence towards risk aversion in traditional communications channels has carried across to the use of social media.

It is little wonder that a simple answer about the use and control of social media within Defence has been difficult to find. The advent of social media is the first point in Defence's history when all worlds collide: brands, organisations, command, members, friends, families, the public, the traditional media and enemies.

Security versus transparency

While conversations are converging in social media, Defence has yet to establish a consistent approach to them. One widely held belief is that members use them only for chatting and engaging with family and friends. Some members view social media use as a highly risky activity that threatens operational security (OPSEC), discloses patterns of life and might bring the Defence brands into disrepute. Others believe that it is beneficial as long as guidelines, including guidance on OPSEC, personal security and the non-disclosure of employment affiliation, are followed.

The conflict between the demands of security and the benefits of transparency creates tension within Defence. An element of resistance among relevant personnel results in a somewhat reactive approach to engaging with the media, in which OPSEC is continually cited as a reason for not engaging proactively. As a result, Defence can sometimes devalue its own positive contributions, forgoing the opportunity to reinforce Australians' pride in the Services.

Marketing and communication versus community engagement

Defence cannot afford to ignore the ways social media can be used in an official capacity. The channel has the ability to deliver the organisation's message without distortion by media interference. Communication in this form allows information to be shared across many platforms and with significant audiences in a more direct and 'human' way. It also allows access to audiences who do not follow more traditional media.

In fact, the Services have already used social media officially and effectively to communicate information about such issues as Anzac Day celebrations, natural disaster recovery assistance, and humanitarian support following the earthquakes in Japan, and to profile service people in their day-to-day activities. Those practices need to be expanded and reinforced to make the best use of social media.

Public relations and marketing play a key role in supporting the actions of Defence and promoting them to the general public. Word of mouth and social media also play their part in maintaining morale, from engaging interest groups to helping Defence members deal with the challenges of distance and separation from family and friends. For many members, social media have become the almost instantaneous replacement for letters home. The new channel should be seen as a vital support to the morale and welfare of Defence personnel and their loved ones.

The new media channels have some special qualities. For example, Defence's most effective social media engagements adopt a much softer and informal conversational tone than the 'corporate speak' used in many press releases and media scrums. Organising responses in social media using traditional communication processes can create difficulties. By their nature, social media call for rapid responses that outpace conventional methods, which may be restrained by detailed approval processes.

Many Defence-oriented community groups that currently share information through other media (such as *Defence Family Matters* magazine) are beginning to establish a presence on Facebook and other social media channels. Some 'presences' are highly targeted and have only a small number of followers, but they can still play their part in supporting the Defence community.

Social media users are themselves potential 'journalists', in that they are able to post comments, stories and other material about Defence matters. The potential benefit of community engagement built through trust and positive connections with users is the promotion of the Defence brands.

Diversity of values and ‘common sense’

Despite efforts to cover social media in policy and training materials, there is much reliance on terms such as ‘professional judgement’, ‘sound judgement’ and ‘common sense’ to describe appropriate social media use. Because such terms are subject to widely varying personal interpretation, they result in a level of systemic risk in the use of social media within Defence.

Some Defence members believe that any misuse of social media can be blamed on Generation Y. Although younger members of Defence and cadets at the Australian Defence Force Academy (ADFA) use the technology more often than others, the vast majority appear to understand, respect and follow the values, code of conduct and guidelines set out by Defence and their respective Services.

There is nothing to suggest that misuses of social media are driven by widespread attitudinal problems; rather, they are only the actions of particular individuals. A lack of training and an overt reliance on terms such as ‘common sense’ to inform behavioural choices may contribute to a misunderstanding of what is expected by the organisation and society. The evidence shows that social media are not the cause of misbehaviour, but simply the conduit for the behaviour. Those who have misbehaved might well have done so using other forms of expression if social media had not been available. To mitigate risks, Defence leadership needs to establish a clear strategic direction for the use of social media and provide appropriate education to reinforce sound behaviour.

Organic growth versus strategy-led innovation

Currently, each of the Services independently manages its own policies and procedures in relation to the use of social media. In the past, the teams managing official social media for the Services established a support network to share knowledge, in conjunction with the Department of Defence Communication and Media Branch. The support group has largely disbanded because of staff turnover, reassignments and roles being unfulfilled for long periods. This uneven resourcing has resulted in some social media presences remaining largely inactive for almost a year.

Many employees using social media as part of their job within Defence have been assigned those responsibilities in addition to their regular workload. Moreover, while some are progressive, self-taught and self-motivated, others with more limited knowledge have been handed the responsibility and appear to be struggling to motivate themselves to meet the incremental workload. There has been relatively high turnover among those tasked with social media management and, as a result, the development of social media presences has been inconsistent.

Currently, the teams are not effectively resourced and lack the specialisations and technology to collect data that can support a business case to the command based on the value of the investment. However, despite being under-resourced in certain areas, the teams are achieving social media engagement that warrants merit.

Defence's social media practices have been developed and tested by lower and mid-level employees, with a focus on tactical execution for external marketing and communication purposes. During this review, it became clear that the general Defence approach to *why* and *how* social media can be used is still in its infancy. As a result, the *test and learn* approach to innovation within the Services has yet to produce a consistent, high-level strategy to develop the channel further. Previous business case submissions for social media monitoring and online metric tools have allegedly been rejected – small teams were primarily responsible for costs, so there was no opportunity to centralise expenditure and deliver such services to all teams currently engaging in social media.

There is limited understanding of social media and their purposes and benefits within the Department of Defence and the Services. Due to the lack of centralised strategy development and visible executive sponsorship, a strategic assessment of the channel, including cost–benefit analysis, has yet to be conducted. A more thorough assessment is needed to identify how to operationalise social media from a human and technological resourcing perspective. The current absence of consistent sponsorship for social media across Defence means there are both a significant opportunity and a need to establish ownership and ultimately take a much more robust and holistic approach to social media, aligned with Defence's overall strategic objectives.

The Defence brands

The review team examined data provided by *BrandAsset Valuator* (BAV) and confirmed something that will be no surprise to the Australian community. The BAV rates all of the Defence Services in the top sixth percentile of all brands in Australia. The Navy, Army and Air Force are some of the most liked, even loved, brands in Australia.

Defence has sound brand values, and Defence personnel understand those values well. They lie at the core of the organisation and the value and belief systems of members. The power of Defence's people as brand advocates and ambassadors is enabling the delivery, in the words of one member, of 'our story, our way', with great effect.

The brand direction of 'people first' currently being used by Defence is an ideal method for engaging the organisation in social media, and this review recommends that this underlying principle remain unchanged. The challenge of this branding method is that, if members of a group are placed at the centre of a communications strategy, any negative action by any members of the group will inevitably reflect more strongly on the brand and the group as a whole. It can be argued that this has been true for Defence in recent months.

Defence has demonstrated that social media can be used as highly effective tools to deliver its messages with honesty and integrity, enabling the ADF and the Services to tell their own stories. Ongoing communication with the general public about aspects of Defence is likely to result in an increase in positive opinion and also achieve results in recruitment and morale.

Channel ownership

If an organisation does not create its own official channel, someone else may create an unofficial one to fill the void. While Defence publicises its official channels, research revealed the existence of dozens of associated sub-brand and related pages. It is unclear whether those pages are official, unofficial, official/unofficial or unofficial/official – all terms that were used by Defence staff to describe them.

This review shows that there are a number of official and unofficial Defence social media presences, and that it is the unofficial pages that have inappropriate content (primarily images). Furthermore, the unofficial presences are not always easily distinguishable from the official ones. There is systemic confusion throughout Defence about what ‘official’ and ‘unofficial’ social media channels are and how they should be used. Clearly defining the types of information and channels that fall into the categories of official and unofficial can produce greater clarity and confidence when individuals participate in social media. In all the circumstances for Defence as a brand, a positive and consistent brand representation benefits the organisation.

Defence personnel should be required to register all social media presences currently being used in an official capacity, in order to establish a centralised database. Administrators of those sites should provide their details so that, as resourcing evolves, continuity plans can be established to ensure that the presences remain active and continue to be managed.

Recruitment

Social media provide an obvious communication channel to engage potential Defence personnel. Many potential recruits are already drawn towards Defence within social media. Currently, they are simply being redirected to Defence Force Recruiting. This is intended to ensure that the potential recruit receives the best advice available, but from a brand perspective it can seem to be slightly dismissive. Initially, at least, direct engagement within the channel is a preferable option to respond to and engage the interest of the potential recruit.

The review team noted that a number of activities by the Services to engage potential recruits via official ADF or Services social media sites (not Defence Force Recruiting) have been highly effective.

Department of Defence – a different brand?

The Department of Defence should consider its approach to official social media differently from the approaches of the Navy, Army and Air Force. The department should consider the resources required, the community’s ability to use this environment to voice alternative opinions, and whether departmental strategy supports the overall goals of Defence. It may well be that the current practice of using the official website rather than social media best fits the department’s role and needs.

Point of failure – reliance on individuals

Communication personnel are monitoring and/or moderating social media manually, in their own time. Their commitment provides significant value for the organisational brands and the organisation as a whole, but this arrangement creates ‘single points of failure’ and is therefore unsustainable. The continuity and consistency of official social media control is vulnerable because it relies on the commitment of the individuals and their availability.

The content and the innovation, responsiveness and overall engagement of some of Defence’s social media presences has merit. It reflects not only the work of the individuals managing those presences on a daily basis, but also the strategic leadership, endorsement and direction from within the broader Defence organisation, although at this stage those contributions are fragmented.

The provision of social media services by individual personnel has created the expectation that the services will be available at all hours. Defence will need to define its commitment to the ‘always on’ aspect of social media.

Content strategy

In social media, content is at the core of all activity – discussions, promotions, photos, articles, links and so on are all content. Defence should view content as an asset that users of the organisation’s official social media can share more broadly with their own networks. Strategy should consider other marketing objectives outside social media and ensure that they are complementary, not contradictory. Defence should also attempt to define the audiences for social media content and tailor the content and location accordingly.

Ideally, a general high-level content plan would be set by an executive committee, a senior social media adviser, or both, in consultation with the communications team for each Service.

Crisis management

Public relations teams are best equipped to generate reactive communication to protect the brands and reputation of Defence. Consistent branding enables audiences to identify information as ‘official’. This is essential during social media crisis management.

However, negative mentions in traditional media do not necessarily drive negative social media conversation. Often, negative coverage can encourage positive conversation, as advocates in social media defend the brand against its positioning in traditional media.

This affects many aspects of the organisation, including policy, operations, management and branding. Issues can escalate quickly in social media, and alignment between offline and online procedures is required to ensure consistency of response. However, at this stage, offline procedures are understood mainly by a few public affairs specialists; high-level documentation would be beneficial when defining online response processes.

Social media policy and guidelines

Definition of social media

Defence does not currently have a clear working definition of social media and an understanding of how they can be used within the organisation. Before reviewing and reworking policy in this area, the organisation should clearly define what social media are in the Defence context, including their content, channels and uses. Throughout the review, the review team found a lack of agreement on the definition and uses of the media. Defining and articulating how they might be used for both official and private communication will be extremely beneficial to Defence in the development of policy and ultimately of training materials for personnel. Defence should articulate what it sees as the role of social media in the organisation, setting out clear parameters for what constitutes organisational, professional and personal use of the media.

Behaviour-driven, evolving and platform-neutral policy

With the rapid evolution of new technologies, policy can become outdated relatively quickly. Moreover, organisations that focus primarily on platforms often ignore the fundamental behaviours underpinning employee communications. Defence should not make that mistake. The organisation's social media policy should remain relatively platform-neutral to ensure that it is scalable and relevant over time. Meanwhile, education and training can complement the policy by addressing the specific mechanics of individual social media policies, such as Facebook privacy settings. The policy should be updated regularly so that it remains relevant, and members need to be made aware of any changes. Defence should also ensure that high-level policy has executive sponsorship and is culturally appropriate in the Australian governmental and legal context.

Inconsistencies in policy

The primary Defence policy guiding the use of social media is *DI(G) ADMIN 08-1 – Public comment and dissemination of official information by Defence personnel*, which was issued on 5 October 2007 and last reviewed on 5 October 2010. Some inconsistencies in the policy have resulted in confusing or ambiguous elements that make it both difficult to understand and difficult to enforce, and Defence's current activities in social media have resulted in ambiguous definitions of official and unofficial commentary. *DI(G) ADMIN 08-1* needs updating to ensure clarity of roles and responsibilities in social media, not only for the broader Defence organisation but also for those managing official social media presences. It should be reviewed thoroughly after Defence sets out a clearer strategy for using social media.

In addition, a number of other relevant policies, such as *DI(G) ADMIN 106 Use of Defence telephone and computer resources*, *Defence Security Manual* and *Protective Security Manual* should be reviewed to ensure consistency, conformance and accountability.

Because Defence uses social media for some official communications, personnel with social media responsibilities will require specific exemptions or alternatives to ensure that the channels can be managed in such a way as not to contravene a one-size-fits-all policy.

Certain legal obligations and directions cannot be fully addressed until Defence clearly defines and agrees on a strategy for using social media. There are foreseeable obligations, such as public records management and archiving, public disclosure, information and operational security and freedom of information, but they will partly depend on the form of the strategy. The proposed Digital Executive Oversight Committee should include Defence legal staff as well as a member of the Government 2.0 Taskforce in an advisory role to provide more detail about legal obligations.

The new policy should set boundaries on the use of social media, whether as part of a Defence member's professional responsibilities or in their personal capacity, to limit the risk of damage to the organisation and other members caused by such use. As Stephen von Muenster states in Section 2.2 of this report:

"A properly drafted and enforced Defence social media policy is the ADF's most effective risk management tool in protecting the organisation from reputational damage and legal liability from the use of social media in during both Professional Use and Private Use."

Defence will need to inform personnel about rules and regulations that supersede the policy embedded in *DI(G) ADMIN 08-1*. This would include social media engagement principles and a broader consideration of personnel's terms of employment and *DI(G) PERS 35-3 Management and reporting of unacceptable behaviour*. With clear parameters for appropriate conduct in professional and private use, personnel can ensure that their behaviour online does not put them in breach of Defence's Values, Code of Conduct or the revised *DI(G) ADMIN 08-1*.

Updating the Defence-wide policy will also require Service-specific guidelines and standard operating procedures (SOPs) to be reviewed and updated in accordance with the revised *DI(G) ADMIN 08-1*. Each of the Services will have slightly different requirements, so each will require modified SOPs for official administrators of its social media sites in addition to SOPs for its personnel. This review also recommends that ADFA review its policy and educational material on social media in order to reinforce appropriate rules and online behaviour for cadets.

Enforcement of policy

The development of a well-defined policy will also aid the commanders and warrant officers who are required to enforce the policy. There is currently a lack of consistent enforcement, which might be a result of inconsistent assumptions about social media and a failure to appreciate the potential risks of misuse. As a result, poor behaviour is often recognised only when more serious infractions are reported in the media or by someone within a social media friendship group.

Feedback from personnel supports the view that monitoring social media practices and enforcement of policy need to be priorities for Defence. Throughout the review, it was noted that most internal investigations into personnel misusing social media resulted from their contravention of other Defence policies, such as those covering bullying, harassing co-workers or breaching OPSEC. Due to the nature of social media, problems can occur with unprecedented speed. While monitoring might not prevent them, it may allow them to be identified early.

Education and social media

Common sense

To date, social media education in Defence has relied heavily on the exercise of ‘common sense’ and ‘professional judgement’. While the organisation may have its own clearly defined views about what those terms mean, they are interpreted subjectively by individuals, some of whom are relatively young, inexperienced, or both. To overcome this problem, Defence should consider reviewing all of its social media training packages to align them with the updated policy. The training materials should demonstrate how the overall and Service-specific policies interlink, and also emphasise the overarching ground rules, such as those covering security and Defence values.

Defence may consider introducing formal training for relevant personnel, which could include training in the tools of social media, realistic guidelines that match the policy, and risk management protocols.

Education and differing audiences

Defence currently has a number of policies related to social media, but this review suggests that the organisation take a more strategic approach to policy development. While central social media policy education should focus on values, principles and guidelines, local social media education should focus on situations in which personnel in a particular Service might find themselves because of their local circumstances. Education and training need to be tailored to different stakeholder groups, according to their requirements, their level of understanding of social media and their rank and position within the organisation.

Applying Defence values

Most personnel already conduct themselves in a manner that is aligned with Defence values and expectations. Each of the Services has already defined organisational goals and values, which should be promoted and used as guideposts for the behaviour of personnel in social media.

Not just OPSEC and not just for personnel

The current primary reason for educating individuals about the use of social media is to support OPSEC, and policy and education are heavily reinforced with Defence personnel before and during deployments. Although heightened restrictions are placed on those deployed overseas, personnel based in Australia should not be taken for granted in regard to the OPSEC, personal privacy and reputational impacts of social media.

Threats to security created by sharing information in social media can never be ignored, regardless of whether a person is based in Australia or overseas. Family members and the wider community also have the potential to put Defence members and themselves inadvertently at risk through the use of social media.

Knowledge of social media privacy issues varies widely within the community. In research conducted for this review, Defence personnel demonstrated a level of inexperience about personal security and privacy in their attitudes towards social media. Overall, the review found that overt reliance on social media privacy settings has led to a false sense of security among those using channels such as Facebook. Those findings were also reflected in survey responses by cadets at ADFA. This problem requires a Defence approach to social media education that addresses security concerns at both the organisational and the personal levels.

Social media education should go beyond Defence personnel to include the wider Defence community. Families and friends should be provided with support and guidelines to communicate safely with their loved ones when using these channels. The guidelines can also be promoted through the Defence Community Organisation, *Defence Family Matters* magazine and Defence Families Australia to reinforce the necessity of protecting family privacy and security.

Integrated training

Personnel indicated to the review team that there is inconsistency across Defence about who provides social media training. In interviews, many stated that the training was relatively ad hoc and that training outcomes could be inconsistent.

As a short-term measure, it would be beneficial to Defence to develop a concise version of the security training guide for social media, which could be used for induction and refresher training for non-deployed personnel. However, the training materials will need to be routinely updated to take into account any changes in policy. In the long term, a complete review of existing education materials and the development of others should reflect the outcomes of the full social media policy review.

Education in crisis identification and escalation

Due to inconsistencies in policy and education, Defence personnel appear to be unclear about how they should identify and escalate a crisis in social media. Therefore, Defence should educate personnel in how to respond (or not respond) to certain types of issues (for example, by using a response assessment tree) and how to escalate a response if escalation is appropriate. While communications staff should receive specialised training and resources to respond to social media crises, other personnel will also require guidance for reporting and escalating concerns about content and activity they see in social media channels.

Operations and social media

Purpose

To ensure that Defence can maximise the potential of social media while minimising the inherent risks from the speed and openness of the channel, it needs to identify and communicate the strategic purpose of using social media. It can begin by asking ‘Why should Defence and its brands use social media?’ Even without thorough guidance from senior command, individuals throughout the organisation are endeavouring to innovate and establish guidelines and SOPs to ensure appropriate use and improve Defence’s reputation online. However, for this channel to function efficiently and effectively, it is important for Defence to establish its vision and purpose for social media centrally, so that those responsible for managing the channel can be confident that their activities are providing value and are supported by the organisation.

Delivering business value – measuring, monitoring and moderating

Because Defence has yet to identify and communicate a consistent strategic purpose for using social media, measuring the effectiveness of the channel has been limited to the gathering of simple statistics, such as numbers of fans/likers and frequencies of page visits. That data does not necessarily produce robust and valuable insights that can be used to advance the business case for using social media. Many results that are reported to the senior leadership of Defence do not resonate or provide significant value.

If Defence can develop a more thorough understanding of why, when and how it uses and should use social media, the teams administering pages online will be able to provide more robust statistics and insights to senior leadership and enable best-practice sharing. It may be beneficial to design and manage a program so that Defence can learn how best to allocate resources to obtain the greatest value for money and support best practice.

Proactive monitoring of social media to identify trends and topics relevant to Defence could profoundly affect the development of proactive media opportunities. The organisation's leadership could then identify threads of conversation or interests that are important to the general public. This would enable Defence to allow the general public and their interests to drive public relations initiatives and ultimately 'shift the conversation'.

Currently, Defence cannot effectively measure its social media successes and failures. By investing in measuring and monitoring technologies, the organisation will be able to benchmark its performance in social media against organisational objectives and key performance indicators.

Service alignment

The individual Services have established their own rules and guidelines for using social media, which has resulted in a somewhat siloed approach to social media policy, education and practice. Public perceptions and the inherently overlapping conversations that occur in social media mean that Defence should have a centralised strategy for social media to ensure the Services' alignment in the broadest sense. Even though strategy and direction would be centralised, resourcing should remain locally based, in order to address the unique needs of the individual Services and ensure responsiveness.

RECOMMENDATIONS

Recommendation 1 (Unified strategy)

Defence should consider establishing a Digital Executive Oversight Committee (DEOC) or similar.

DEOC will provide executive sponsorship and guidance to ensure that Defence's social media strategies and tactics are aligned.

It would be beneficial to Defence if DEOC were chaired by a senior member of the organisation. That would add gravitas to the group's practical and inspirational leadership roles.

The committee should have a balanced representation from across Defence, including Communications and Media Branch, ICT, Human Resources, the Defence Community Organisation and Intelligence.

While strategy and direction would be centralised to DEOC, resourcing should remain locally based in order to address the unique needs of the individual Services. Should Defence attempt to centrally coordinate all social media activities, it would run the risk of creating approval bottlenecks that could undermine the speed and authenticity of the conversation and engagement. Organising social media requires a hybrid approach to management, with top-down leadership influencing medium- and long-term strategy and policy, but decentralised day-to-day execution.

DEOC would ensure that efforts in social media are focused on, but not limited to:

- assessments of social media and strategy development
- cost–benefit analyses
- expenditure and resourcing control
- best practice documentation and dissemination
- the education of senior personnel
- the setting of Defence's social media education agenda
- establishing and maintaining a register of all official and associated social media sites.

Recommendation 2 (Policy)

All policies relating to the use of social media, the internet or cyber-activities should be reviewed. Services guidelines should also be reviewed to ensure that they are consistent with the overall social media policy and engagement principles.

Although the Services have different individual requirements, they should collaborate to ensure broad consistency in their guidelines. This could be coordinated by DEOC.

Clear social media guidelines should be brought to the attention of individuals at the point of engagement with Defence in social media.

A policy identification decision tree or process should be developed to help members navigate to relevant information without expecting them to have a full understanding of all policies.

Recommendation 3 (Education)

Defence should consider reviewing social media training and the way it is prioritised and delivered in order to ensure consistency. The review should include relevant resources, guidelines and support mechanisms.

Education and training should be tailored to different stakeholder groups according to their requirements and level of understanding of social media. For example:

- Executive-level training should focus on education about the opportunities and risks associated with social media, as well as on opportunities to contribute to DEOC.
- Middle managers should be equipped with the skills and knowledge to support and help implement social media practices within their local areas.
- Personnel should be trained about the use social media to ensure responsible representation of themselves and Defence, and about how they should access relevant policy and guidelines.

The training should align with the updated policy and a single vision defined by DEOC to ensure that a *balanced* education is delivered.

All training materials should demonstrate how the central and local policies interlink and should also emphasise overarching ground rules, such as security and Defence values. All training should be well defined, with actionable take-outs, use sound examples, and place limited reliance on the application of ‘common sense’.

Once social media have been defined and inconsistencies in policy and education have been resolved, Defence may wish to develop a platform-neutral decision tree or guide to help personnel locate the social media policy section appropriate to their situation. The guidance should provide high-level guidance to personnel, rather than guidelines for every scenario that might arise.

Social media education and support should go beyond Defence personnel to include friends and families.

Recommendation 4 (Resourcing)

Human and software resources should be defined and provided to support the understanding and management of social media in Defence.

Resources could include incremental specialised personnel, software to monitor, measure and understand online activity, and engagement and moderating tools.

DEOC should administer centralised expenditure for resources and monitoring and moderation software, as this process will benefit a number of areas of Defence.

Recommendation 5 (Channel/content plan)

Defence should investigate the benefits of aligning content strategies across official social media.

Local social media teams should define and share content strategies and consider predefined plans, such as a five-day calendar of events for each working week.

Defence and Defence Force Recruiting should continue the ‘test and learn’ methodology within official Defence social media presences. Further consideration should be given to the effects of immediately deferring recruitment enquiries made in the social media space.

Recommendation 6 (Crisis management)

Defence should develop a social media crisis plan that aligns with existing PR, marketing and brand communication plans.

Although crisis management is usually reactive, a plan could be developed in conjunction with key stakeholders to consider proactive strategies as well.

As part of the plan, Defence should define what constitutes a crisis and identify specific types of breach and the best responses to them. A triage system for assessing risks according to probability and severity could be used, which would help to mitigate problems in the social media space before they become crises.

During a crisis, Defence should adopt a more assertive and faster paced process, as outlined in the introduction to Section 4 of this report.

Personnel tasked with managing social media should receive special training in how to respond to a crisis quickly and flexibly. Fast-tracked approval processes should be implemented to enable them to address the crisis in good time. Other personnel will also require guidance on how to react.

High-level documentation on the specialist practices, processes and procedures currently used in crisis response management should be prepared, in order to align a similar process for social media.

Recommendation 7 (Brand)

Defence should maintain its current brand direction of ‘people first’ in its social media activities.

This review was tasked to define a brand strategy to enhance Defence’s brands in social media. The review team believes that the brand direction of ‘people first’ currently being used in Defence is the ideal method for engaging in social media. The pursuit of that underlying principle should continue.

OVERVIEW

On 6 May 2011, the Honourable Stephen Smith MP, Minister for Defence, announced that the Australian Government would undertake a number of comprehensive reviews following allegations of inappropriate conduct at the Australian Defence Force Academy (ADFA) and inquiries into what the Minister called the ‘ADFA Skype incident’, which occurred in March 2011. A steering committee chaired by the Vice Chief of the Defence Force would coordinate the work of the reviews.

Mr Smith announced that five inquiries would be undertaken, in addition to the review of the ADFA Skype incident and its management. One was to be a review of social media use in Defence, which is the subject of this report. In relation to this review, the Minister said:

The impact of social media has created new challenges for the ADF and the Defence organisation. The review will examine Defence’s obligations in relation to the use of social media by its employees and the organisation, and make recommendations to mitigate associated risks and to harness opportunities to improve Defence’s work and reputation.

(Department of Defence 2011)

The Minister also said that the review would aim at developing measures to ensure that the use of social media, in this context, is consistent with Defence values.

In particular, this review is responsible for auditing Defence’s current and foreseeable obligations in the future, assessing relevant attitudes and practices of Defence personnel, examining international best practice in this area, and providing an implementation plan for Defence to meet its obligations and implement best practices.

This comprehensive review of the use of social media and Defence is the first of its kind. It provides a background to current local practices and attitudes in Australia, as well as in defence forces closely allied to Australia. The review also provides an opportunity to assist Defence with a blueprint for developing practices, procedures and protocols that are relevant not just to the current needs of the organisation, but also to meet its future needs in the ever-changing and adapting online environment.

TERMS OF REFERENCE

Aim

1. The Review is to examine Defence's obligations in using social media in order to achieve Defence outcomes, including the recruitment and retention of prospective employees, and make recommendations to mitigate associated risks and to harness opportunities to improve Defence's reputation.

Background

2. Social media, those online technologies that enable people to communicate and share information and resources via the internet, is changing people's ideas about privacy, information security and organisational control. The ubiquity and penetration of social media is also changing social attitudes, community values and the interactions between individuals and their workplaces. Social media has different impacts across the generations. For those in 'Generation Y' and younger, social media has different implications and is creating different expectations than for 'Baby Boomers' and 'Generation X'.
3. For Defence, the impact of social media and the changing expectations and social mores of younger generations creates new challenges including in the areas of information and operational security, workplace safety and reputation. Defence needs to understand the expectations and mores of current and prospective employees. Changing technology and community expectations has the potential to create unexpected organisational impacts, which Defence must anticipate and work towards building effective responses for. We must ensure that new technologies and social attitudes benefit our people, promote Defence values and support our core roles and functions. We must adapt our policies, procedures, training and recruitment models to acknowledge the increasing use of social media by our current and prospective employees and ensure that we respond effectively to mitigate risks and to harness opportunities.

End State

4. The review will deliver four elements:

a. Firstly, an **audit of Defence's extant and foreseeable obligations**, as a government department, a military organisation and as an employer, relevant to the use of social media by Defence and its employees (such as privacy, equity and diversity, information and operational security, freedom of information, freedom of speech, public records management and archiving, public disclosure and accessibility).

b. Secondly, an **assessment of relevant attitudes and practices** of current and prospective Defence employees in relation to social media and related technology and an assessment of Defence's current presence in social media. This examination would include:

(1) analysis of the impacts and effectiveness of current social media activities in Defence, including DFR digital marketing services;

(2) analysis of the impacts and trends of social media on youth culture and social mores; and

(3) analysis of patterns and trends in the use of social media and related technologies across key age cohorts.

This component would also provide an analysis of Defence's presence in the social media and perceptions and attitudes of the Australian community that stem from this presence.

c. Third, an **assessment of international best practice** (with consideration of US, UK and Canadian military forces) in:

(1) mitigating and responding to misuse of social media by employees; and

(2) harnessing social media for 'branding' and meeting public obligations.

d. Finally, deliver an **implementation plan** for Defence to meet its extant obligations and to achieve international best practice in social media policy. We would expect such work to address options to:

(1) explain and promote appropriate use of social media by current employees;

(2) mitigate and respond to misuse of social media by employees; and

(3) make better use of social media for:

i. meeting government obligations,

ii. enhancing Defence's brands and public reputation, and

iii. engaging with and supporting its workforce.

5. The review is to take account of:

- a. the Government's response to the Government 2.0 Taskforce;
- b. the commitments of the Government to enhancing the Australian Public Service discussed in the report 'Ahead of the Game: Blueprint for the Reform of Australian Government Administration';
- c. the social media initiatives of Defence, such as iArmy, and other Defence initiatives which leverage off social media such as DefenceJobs;
- d. relevant Departmental policies in the area of information security, public commentary and engagement with the media, and equity and diversity; and
- e. work undertaken within the Department, including that done by our forces in the Middle East Area of Operations with respect to deployed Defence personnel and social media.

6. The review will consult widely with both Defence personnel and the Australian community to gauge the community expectations of Defence's interaction with social media and new technology.

Governance

7. The review will be conducted under the auspices of the Defence Steering Committee established to oversee a number of related reviews, including on women in Defence. The Deputy Secretary for Strategy acting as Defence's lead senior contact point for the external reviewer.

8. Defence will provide suitable resources to support the review, which will be managed by a Secretariat reporting to the Steering Committee. The reviewer will have access to Departmental officers as required and a small budget for travel and other necessary pre-requisites.

9. The completed review will be provided to the Defence Steering Committee. The review and a proposed defence implementation plan will be provided to the Minister for Defence for his consideration. Subject to the Minister's views we would expect that the review and any Defence response will be made public.

Conduct of the Review

10. The Review will be conducted by a team from George Patterson Y&R (GPY&R), led by Rob Hudson (Head of Digital).
11. GPY&R will conduct the following four tasks, concurrently:
 - a. an audit of ADF's extant and foreseeable obligations - this phase will act as a scoping phase and this may affect the subsequent areas of work in relation to deliverables and head hours. Regular communication and updates will be provided to manage the scope of work;
 - b. an assessment of relevant attitudes and practices regarding social media (both within Defence and in the Australian society more broadly);
 - c. an assessment of international best practice for overseas military forces and other relevant organisations; and
 - d. an implementation plan for Defence to mitigate associated risks and to harness opportunities to improve Defence's work, reputation, and outcomes.
12. The GPY&R activities will be supplemented by two discrete pieces of further analyses:
 - a. The first of these is an internal audit of Defence's extant and foreseeable obligations, current policies, procedures and practices. This analysis will:
 - (1) audit Defence's extant and foreseeable obligations as a government department, a military organisation and as an employer relevant to the use of social media by Defence and its employees;
 - (2) detail Defence's current social media policies, procedures and practices;
 - (3) identify steps already taken in theatre and at the operational level as a consequence of previous Facebook issues; and
 - (4) identify the principal Defence challenges in the social media environment.
 - b. The second analysis will be conducted by an academic working in the social media context. This analysis will be a sociological analysis of the impacts of social media technologies on the broader Australian population, with particular consideration of the various commonly-used age brackets (14-18, 18-25, 25-45, and 45+). This analysis will support the work of GPY&R through provision of an academic analysis of ubiquity and penetration of social media and the consequential impacts of social media on Australian social attitudes, community values and the interactions between individuals and their workplaces. As a more generalised analysis of social media from an Australian community perspective, this element of the review will provide important framing for the issues that Defence must manage with respect to its workforce and engagement.

Report

13. The review report will be completed by 30 July 2011.

CONDUCT OF THE REVIEW

This review is a composite of research, observations and findings by the review team at George Patterson Y&R. This is a synthesis report, in that it is accurate about the material relied upon, organised in its approach and interprets the analysis and research data in accordance with the terms of reference, in order to provide a well-rounded and greater understanding of social media and its place in Defence.

The review team at George Patterson Y&R referred to and considered the following sources in order to develop its findings, conclusions and recommendations and prepare this report:

- general research on the various subject areas relevant to the review
- examination and assessment of international social media policies, strategies and protocols, using material produced by the armed forces of the United States of America, the United Kingdom, Canada and New Zealand
- quantitative and qualitative research to gauge attitudes, perceptions and views about social media, both in the general community and within the Defence organisation.

RISKS AND LIMITATIONS

The timeframe for this review was short. Given the need to examine and review international and local documents and to conduct quantitative and qualitative research, completing those tasks in the available time was challenging. The review team acknowledges that time limitations have meant that not every avenue has been pursued. However, the team was able to reach both general and specific conclusions from the material examined in the time available, resulting in the findings and recommendations in this report. The findings can be a platform for further investigation by Defence.

The review was restricted to some extent by some limitations in the current bodies of knowledge held by Defence. For example, no comprehensive list of official social media sites exists and there are limited human and financial resources for social media, which means that identifying all specialist points of contact is a complex task.

There is always a practical limitation when reviewers are external to an organisation. On the one hand, they are not bound by organisational culture; on the other, ‘outsiders’ need to quickly understand the nuances of a culture in order to properly assess it and earn the trust needed to allow sources and participants to feel comfortable when cooperating with the review. While the review team did not encounter notable resistance, it must be recognised this review was created on the basis of a ministerial instruction.

As a result of security and practical considerations, Special Services were not consulted during the review, but it seems likely that the attitudes, perceptions and cultural usage of the medium found by the review team are reflected throughout the Defence organisation. The extensive research conducted by the review team shows a continuum of views in Defence, and the review provides a broadly representative flavour of views within the organisation.

Both Facebook and Twitter limit historical access to posts and updates, so the review team has based its findings on the content available during the audit period and on the quantitative and qualitative research in support of the review.

STRUCTURE OF THE REVIEW

The review team has been conscious of the terms of reference and related questions about social media that the Minister and other stakeholders want examined. To that end, its approach has been to present the relevant information, provide reliable findings and make effective recommendations.

Section 1 of this report (Social media and their origins) examines the meanings of ‘culture’ and ‘social media’ and looks at the abundance of meanings for the latter term. While definitions abound, it is helpful to fit the most commonly used forms of social media into six categories, four of which are referred to often in this document.

Section 2 (Trends, legal obligations) examines a number of issues to do with social media and its place in the current context. They include an assessment of the current trends of social media use in the armed forces and the community generally; an investigation of the legal obligations related to social media use and Defence.

Section 3 (Analysis and insights) examines social media and Defence through the triple bottom line of management, morale and marketing. Within each of those strands, international best practice, Defence practices and attitudes, and insights on the material are discussed.

Section 4 (Strategy and Implementation) also uses the triple bottom line, but in this case to examine the themes of social media policy strategy, employer social media brand strategy and social media problem mitigation and response. The section provides insights into where social media policy and Defence might move in the future.

Three annexes to the report present qualitative and quantitative data about social media in Defence and the wider community, and examine public perceptions of social media and Defence.

SOCIAL MEDIA AND ITS ORIGINS

This review was predicated on two elements: first, it was a *cultural* review; second, it examined the issue of *social media* and Defence. This section of the report explores both concepts.

1.1 WHAT IS CULTURE?

The word ‘culture’ is commonly used to denote many varied aspects of society, sometimes without much thought about the meaning of the term. Definitions developed by researchers give some insight into what ‘culture’ might mean for an entire society, or groups within that society, such as Defence.

The published research of Geert Hofstede, who surveyed the cultural attitudes of more than 116,000 IBM employees in 50 countries and three regions, is regarded as seminal, particularly when scholars assess how national culture affects workplace culture (Mead 2002:39). The principal purpose of his analysis was to differentiate between the assumed ‘shared’ values held in organisations and the ‘unique’ values that could be identified as belonging, instead, to national cultures (Mwaura et al. 1998:214).

Hofstede argued that culture can be regarded as ‘the collective programming of the mind which distinguishes the members of one group from another’ (1984:21). Later, he added that culture can be ‘mental programming ... patterns of thinking and feeling and potential acting’ (Hofstede 1991:4).

Many others have also provided definitions of ‘culture’. For example, Hoebel and Frost say culture is an ‘integrated system of learned behaviour patterns which are characteristic of the members of a society and which are not the result of biological inheritance’ (1976:6). Ferraro (2002:19) argues that it is ‘everything that people have, think, and do as members of society’. Samovar and Porter (1991:51) describe culture:

as the deposit of knowledge, experience, beliefs, values, attitudes, meanings, hierarchies, religion, notions of time, roles, spatial relations, concepts of the universe, and material objects and possessions acquired by a group of people in the course of generations through individual and group striving.

Hill (2003) sees culture as being ‘social structure, political system, economic philosophy, religion, language and education’.

One striking difference between these definitions is that the last two describe what might be seen as the constituent parts of a culture, whereas the others attempt to define the term.

Dwyer (2009:36) argues that culture operates at three levels. At the first level it is visible, and can be defined as obvious patterns and behaviours, along with technology, buildings and artefacts. The second level is less visible and involves cultural communication; that is, how people communicate both verbally and nonverbally. At the third level it is made up of the 'ideas, basic assumptions, values and beliefs held by a society' and is almost invisible.

If communication can be divided into three realms of words, material things and behaviour (Hall & Hall 1990:3), then social media provide an interesting and complex challenge, as they bridge the three levels of culture and communication.

Jones (2007:3) argues validly that culture is not easily acquired and is a slow developing process, supporting the argument that it is a type of 'programming'. Not surprisingly, cultural attitudes need to be taken into account because of their great resilience, fuelled by their origins and inherent reinforcing dynamics (Peterson 2007:372). If culture is slow to develop and integral to the society and its members, that also means that it is resistant to change.

By extension, Defence personnel generally reflect the cultural attitudes of the society from which they emerge. Of course, organisations develop their own cultures, which influence those who work with or within them. The individuals then negotiate for themselves those aspects of the organisational culture that they can accept within their value and belief systems and those they cannot. Whether an organisation is a local social club, a business, a government department or a defence force, it will develop accepted cultural views that inform the behaviour of its members.

Defence's organisational culture is born of need, tradition, the armed forces' position in society and their unusual work.

General Australian cultural attitudes and those values and attitudes specific to Defence must both affect attitudes to the use of social media. For obvious reasons, this can create conflict from time to time. The conflict will be exacerbated by generational differences, particularly as technology changes the way people communicate and interact with one another, and perhaps also by regional or other differences. In addition, users of social media participate in an online culture that is still developing.

Those inducted into the Defence organisation need to negotiate cultural values at all these levels.

1.2 What are social media?

The rapid development of both technology and the skills and knowledge of social media users means that what makes up 'social media' continues to change at a rapid rate, as new websites and online content appear each day. As Jacka and Scott (2011:5) argue, 'there is no single recognized definition of social media.'

For many people, well-known social network sites such as Facebook and Twitter typify social media. The sites have become enormously popular across demographics of race, age and gender, and have hundreds of millions of users.

Jacka and Scott (2011:5) contend that it 'can be said that social media is the set of Web-based broadcast technologies that enable the democratization of content, giving people the ability to emerge from consumers of content to publishers'. The *Oxford Dictionary* (2011a) defines social media as 'websites and applications used for social networking'. In turn, social networking is defined as 'the use of dedicated websites and applications to communicate with other users, or to find people with similar interests to one's own' (Oxford Dictionary 2011b). For many this will intuitively make sense, based on their personal experience, the experience of others around them, or what they have heard or seen in the media. However, social media have evolved to include other tools and practices that were not conceived of only a few years or even a few months ago.

The ABC (2011) has produced a Technology Explained website, where definitions and explanations are provided for modern technical and online terms. The website comments that:

'Social media encapsulates digital tools and activities that enable communication and sharing across the net ... Social media is used prolifically by all areas of society; business, politics, media, advertising, police and emergency services. It has also become a key tool for provoking thought, dialogue and action around particular social issues'.

The Social Media Guide website (2011) has listed some 50 definitions that it says it has collected from various other websites. In its terms, 'social media is user generated content that is shared over the internet via technologies that promote engagement, sharing and collaboration.'

Kaplan and Haenlein contend that social media as we know it today can probably be traced back more than two decades. While it was unsophisticated by today's standards, users could post public messages on sites such as Usenet. Not surprisingly, the advent and availability of high-speed internet access has led to a proliferation of sites and an explosion in their popularity (Kaplan and Haenlein 2010:60).

Kaplan and Haenlein (2010:61) developed their own technical definition of social media:

'Social Media is a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content.'

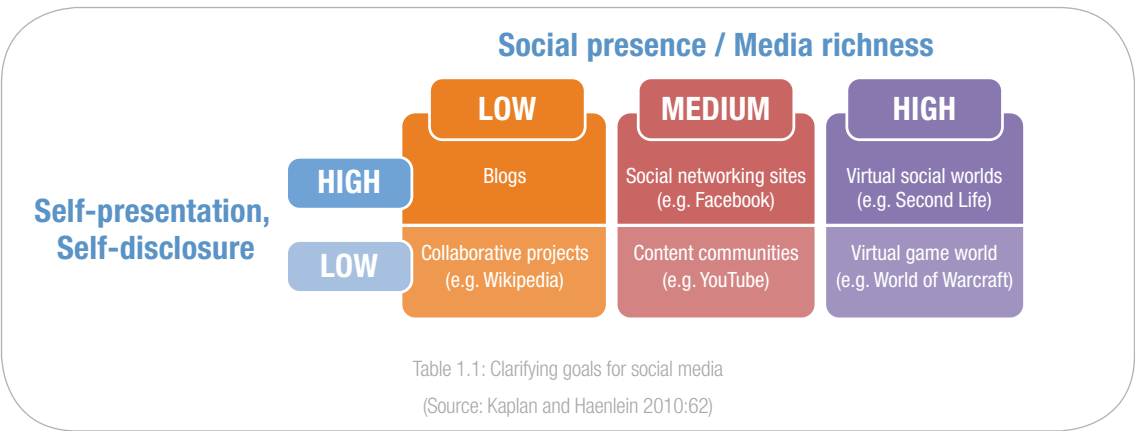
Web 2.0 is described ‘as a platform whereby content and applications are no longer created and published by individuals, but instead are continuously modified by all users in a participatory and collaborative fashion’, so Web 2.0 might be seen as the ideological and technological foundation of social media. The mere publishing of content is less interactive and belongs to the earlier Web 1.0 era; collaborative projects, starting with blogs, belong to Web 2.0 (Kaplan and Haenlein 2010:61).

User-generated content (UGC) describes the various forms of media content that are created by and available to users. Kaplan and Haenlein (2010:61) go further and adopt the view of the Organisation for Economic Cooperation and Development that content must meet three basic requirements to qualify as UGC:

- It must be published to all Web users or to a select group (which might exclude emails or instant messages).
- It should demonstrate some creative effort and not simply replicate the work of another.
- It must be created outside of professional routines and practices and not for a commercial market.

Although UGC was available before Web 2.0 emerged, the combination of technology, economics (wider access to the tools of creation) and social influences (the rise of a generation of ‘digital natives’ and ‘screenagers’) has driven its development (Kaplan and Haenlein 2010:61).

Kaplan and Haenlein (2010:61) further argue that the development of a systematic classification scheme for social media can be difficult, as new sites appear every day. They rely on the field of media research and have decided that social media have two key elements that can be used to classify them to some extent: social presence / media richness on the one hand, and self-presentation / self-disclosure on the other. To demonstrate, they have combined the two classifications into a table that illustrates their arguments (Table 1.1).



The table shows how different types of social media involve different commitments from the user. For example, a person who wishes to become a fully involved user in a virtual social world, rather than merely adding daily textual additions to their blog, would in a general sense disclose more about themselves (whether consciously or not), and their online presence would necessarily require a more involved use of media tools.

Kaplan and Haenlein's categorisation of social media is adopted here to enable discussion about the various types:

- **Collaborative projects** enable the joint and simultaneous creation of content by many users. Examples include various 'wikis', such as Wikipedia. Some of these sites allow users to add, remove and change content; others are a form of 'social bookmarking', in that they allow the group-based collection and rating of internet links or media content.
- **Blogs** – the earliest form of social media – grew from personal web pages and usually display date-stamped entries in reverse chronological order. Text-based varieties are still very popular.
- **Content communities** have as their main purpose the sharing of media content between users, including text (e.g. Bookcrossing), photographs (Flickr), videos (YouTube) and PowerPoint presentations (SlideShare). Users are not usually required to create a personal profile page.
- **Social networking sites** allow users to connect by creating personal information profiles and inviting friends and colleagues to have access to the profile and to send emails and instant messages. Profiles usually include photographs, videos, audio files, blogs and so on. Facebook and Myspace are examples of social networking sites.
- **Virtual game worlds** are platforms that replicate a three-dimensional environment in which users appear in the form of personalised avatars and interact according to the rules of the game. They have gained popularity with the support of devices such as Microsoft's XBox and Sony's PlayStation. An example is World of Warcraft.
- **Virtual social worlds** allow inhabitants to choose behaviour more freely and to live (in the form of avatars) in a virtual world similar to their real life. An example is Second Life.

This review concentrates on the first four categories and not the two types of virtual world. It is likely that the common experience of most Australians, including Defence personnel, in social media is in the first four categories and, in any case, the lessons to be learned from the first four can be extrapolated in many ways to apply to the latter two groups. In addition, the virtual game and social worlds are very specialist and large in scope and would require their own specific examination.

Much of the time spent in social media by Australians is on social networking sites (see, for example, the discussion about Facebook use in Section 2.1). A definition by Boyd and Ellison (2008:211) expands on the definition of social networking sites given above:

‘... web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site.’

They go on to say that what makes the sites unique is not that people can meet strangers, but that they will have a visible social network, which can result in connections with strangers, although that is not often the goal. The sites allow someone to display a public profile, which may show a network of ‘friends’ with whom they have made a connection. The user is able to publish text, comments, photographs and multimedia content to that profile. Sites vary with the security settings users set for their profiles, which variously allow others to access the profile and the material they have posted to the site.

Social networking sites might seem a recent innovation, but there is plenty of evidence to the contrary. Section 2.1 includes a timeline that supports the view that there is a cycle of popularity for these sites, as new ones with new features come online.

Social media will continue to evolve by adapting to the demands of users, making any attempt to fully define the term problematic. However, they are likely to become even more all-encompassing and be embraced more strongly by generations to come.

TRENDS AND LEGAL OBLIGATIONS

Before analysing the current position of social media within Defence and offering suggestions about strategy for enhancing the organisation's response, it is necessary to establish a baseline of general data and information.

This section is in two parts, each with a logical part to play in that task:

2.1 Trends

This section examines social media trends in Australian society in general, who is using social media and what they are using it for. It discusses sites that are attracting attention, and a timeline shows the global evolution of social network sites. The section also looks at some recent success stories, when social media have acted as conduits in times of crisis.

2.2 Legal obligations

This overview examines the laws that may influence and restrict Defence participation and engagement in social media. It is a high-level examination primarily of Defence and its members' engagement with a broad internal and external community of organisations and individuals that are interested in the activities of Defence. In considering social media use from a legal perspective, this section offers suggestions for 'engagement principles'.

2.1 TRENDS

Australians' interest in and use of social media have increased over recent years. Since 2009, we have been among the world's heaviest users of such sites. The trend towards going online and communicating via the internet has meant that social media have become a part of everyday life for many, but youth are the highest consumers in terms of usage, frequency of use and time spent online. The integration of social media into life has affected a wide variety of societal aspects, including news reporting, technology, crisis communication, privacy, and even what it means to be someone's 'friend'.

2.1.1 Trend: Australians among the heaviest users

The global social media landscape has evolved rapidly over the past five years. The use of social media has become a mainstream activity and arguably part of the everyday life of many people. The number of Australian internet users aged 14 and over who went online during the December quarter of 2010 was approximately 15.1 million, up from 14.2 million for the same period in 2009 (ACMA 2011:2). According to comScore (2011), social networking 'accounts for 1 in every 5 minutes spent online in Australia'.

By the end of 2009, Australians had become some of the world's heaviest users of social media, spending an average 6 hours and 52 minutes a month on social sites (Table 2.1).

Country	Unique Audience (000)	Time per Person (hh:mm:ss)
United States	142,052	6:09:13
Japan	46,558	2:50:21
Brazil	31,345	4:33:10
United Kingdom	29,129	6:07:54
Germany	28,057	4:11:45
France	26,786	4:04:39
Spain	19,456	5:30:55
Italy	18,256	6:00:07
Australia	9,895	6:52:28
Switzerland	2,451	3:54:34

Source: The Nielsen Company

Table 2.1: Internet use in 2009, by country
(Source: The Nielsen Company 2011)

The frequency of consumption of social media by Australians is evident in the Sensis social media report (Sensis 2011), which was targeted at social media users and conducted through phone interviews. Some 30% of survey participants made use of social media every day, with an overall average for all survey participants of 12.4 times per month (Figure 2.1).

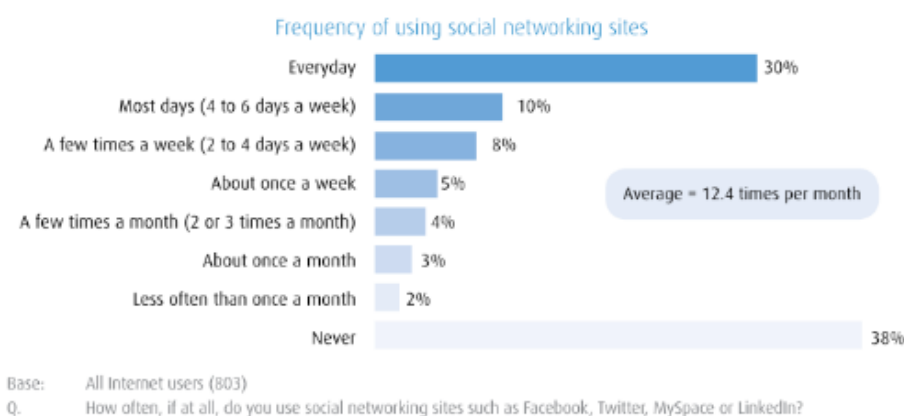


Figure 2.1: Frequency of using social networking sites
(Source: Sensis 2011:10)

The Sensis report further segmented the frequency of use of social networking sites by age and gender, as shown in Table 2.2.

Social networking site usage by age and gender

	Total (803)	Male (402)	Female (401)	14-19 (100)	20-29 (140)	30-39 (134)	40-49 (135)	50-64 (160)	65+ (134)
Everyday	30%	25%	36%	70%	52%	39%	14%	15%	5%
Most days	10%	9%	11%	15%	20%	9%	11%	5%	3%
A few times a week	8%	8%	8%	7%	12%	10%	7%	7%	5%
Once a week	5%	6%	5%	1%	6%	6%	5%	5%	8%
Less than weekly	9%	10%	7%	0%	4%	9%	22%	5%	10%
Never	38%	42%	34%	7%	7%	27%	41%	64%	69%
Average times per week	12.4	10.6	14.1	24.9	21.4	15.2	7.9	6.5	3.1

Base: All Internet users
Q. How often, if at all, do you use social networking sites such as Facebook, Twitter, MySpace or LinkedIn?

Table 2.2: Social networking usage, by age and gender
(Source: Sensis 2011:10)

It is evident from Table 2.2 that 14–19-year-olds are the most frequent users of social networking sites; some 70% of those surveyed in this age group stated that they accessed such sites every day. The second most frequent users are 20–29-year-olds; 52% of those surveyed indicated that they used social networking sites every day. This is an important finding for organisations that have a need or desire to target ‘youth’. The survey results indicate that more than 59.5% of 14–29-year-olds access social networking sites every day, indicating that social networking sites are key channels for sending messages to young audiences (Sensis 2011). While the number of survey participants in each age demographic was not high, there is nothing to suggest that the results are not broadly reflective of the overall population of social media users.

It is also important to determine which social media sites experience the highest frequency of usage by Australians, in order to understand the best platform for communicating with them. The data in Figure 2.2, taken from this review’s public survey, shows that the most frequently used social media site was Facebook; 32% of respondents said they used it several times a day, and 99% of respondents were aware of the site.

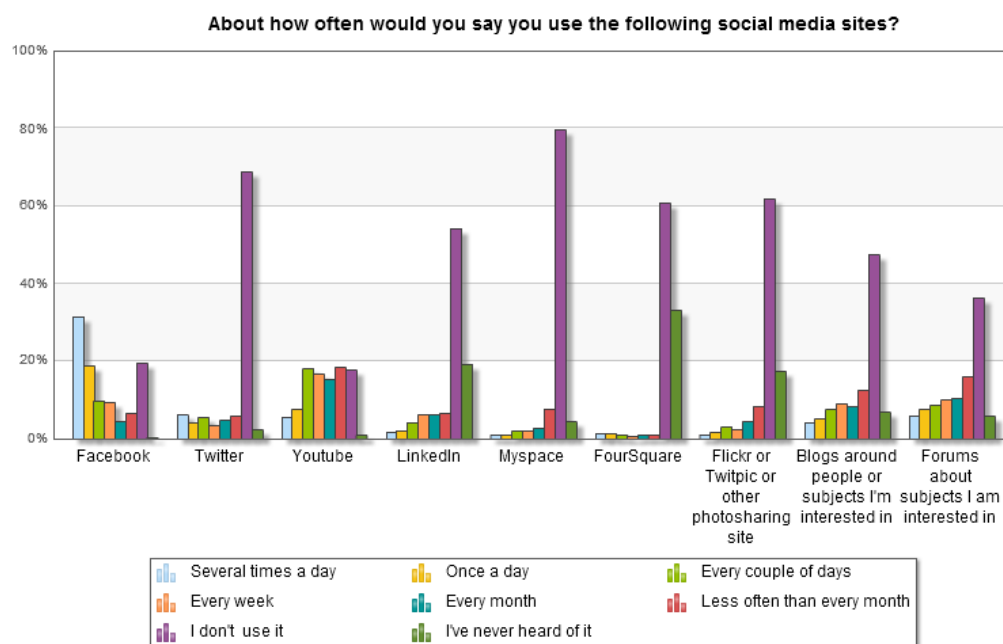


Figure 2.2: Use of social media by the general public, by site

2.1.2 Trend: Social media during natural disasters

In 2011, social media became increasingly important places for Australians to turn to in times of natural disaster. In January, Queensland experienced flooding in many areas, including Toowoomba and Brisbane. When the Brisbane City Council (BCC) website crashed due to an overload of traffic, the council used Facebook and Twitter to send information about, for example, areas being evacuated and those that were flooded. The public responded by 'liking' the BCC Facebook page and/or following the BCC Twitter account in order to remain informed about the unfolding crisis. The Facebook page had 761 likes at the beginning of January but 12,648 by the end of the month.

BCC was not the only entity that used social media to communicate during the floods. The Queensland Police Service (QPS) also used them to communicate with the public and to correct false rumours. The community needed timely, relevant and accessible information, and that was provided through social media. According to Larkin (2011), the QPS Facebook page went from under 25,000 likes to 165,000 likes during the floods. The QPS Twitter account (@QPSMedia) used the hashtag **#mythbusters** to deal with misinformation or disinformation during the crisis. QPS's Facebook page dealt with false information in a similar way. This obviously helped to ensure that the general public were up to date with all information (including false information).

Although the QPS broadcast information about the hardest hit areas, residents in local communities were looking for more localised material, relevant to them. Where local or regional councils did not provide that information, communities created their own social media platform to discuss and share their experiences of the floods. The community took the responsibility for information into its own hands: several 'area' or 'shire' pages surfaced, such as the Caboolture Shire and Surrounding Suburbs Floods page (Figure 2.3).

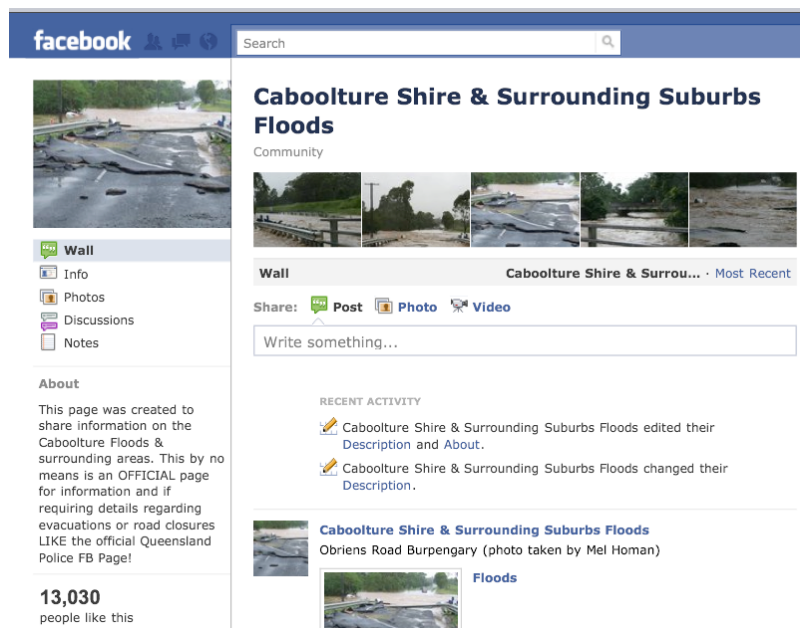


Figure 2.3: Caboolture Shire and Surrounding Suburbs Floods Facebook page
(Source: Facebook, 15 July 2011).

The page was created by a member of the community to publish:

- photos of flooded or damaged areas
- requests by the community for help
- offers to help or donate materials
- updates on what roads were open or closed
- information about official channels
- criticism of the regional council for not setting up a page similar to those created by the QPS or BCC
- false rumours about the floods, some of which were corrected by fellow community members.

People who lived outside the affected communities also used the page to check whether family and friends were safe. The page had approximately 13,000 likes by the end of the week of the floods.

Another example of the use of social media during times of natural disaster was during Tropical Cyclone Yasi, which crossed the North Queensland coast on 3 February 2011 (Colgan et al. 2011). This natural disaster was not centred on a metropolitan area, so different methods of communication were used to communicate with people who were or would be affected by the cyclone. Social media played a part in getting information about Yasi to the public outside the affected areas.

A Twitter account, @cycloneupdate, was established by a local weather enthusiast, who monitored cyclone activity and broadcast it to the world. The owner of the account was approached by media outlets requesting interviews, and the information provided by this unofficial source was even retweeted by major news outlets (Figure 2.4).



Figure 2.4: ABC News retweets unofficial '@cycloneupdate' post
(Source: Twitter, 1.18 pm, 2 February 2011)

Social media are becoming an important part of crisis management for governments and communities, particularly during natural disasters. Where the authorities are not communicating through Facebook and Twitter, the community creates an information and content sharing environment, using social media to fill the gaps.

2.1.3 Trend: Conversation drives interaction

Before Facebook, it was Myspace, and before Myspace it was Friendster – social media is about people and their need and desire to communicate, not specific platforms (which so far have been transitory). This is a critical factor when formulating and implementing social media policies and regulations covering social media behaviour: social media usage is driven by people's need to converse and interact.

According to the Sensis report (2011), the main reason Australians use social networking sites is to catch up with friends and family (Figure 2.5). Conversing with friends online can be as important as communicating offline, particularly for people separated by distance. Social media allow users to create a life and personality online, which often reflects their offline presence. Social networking can be seen as a digital extension of the 'real' self.

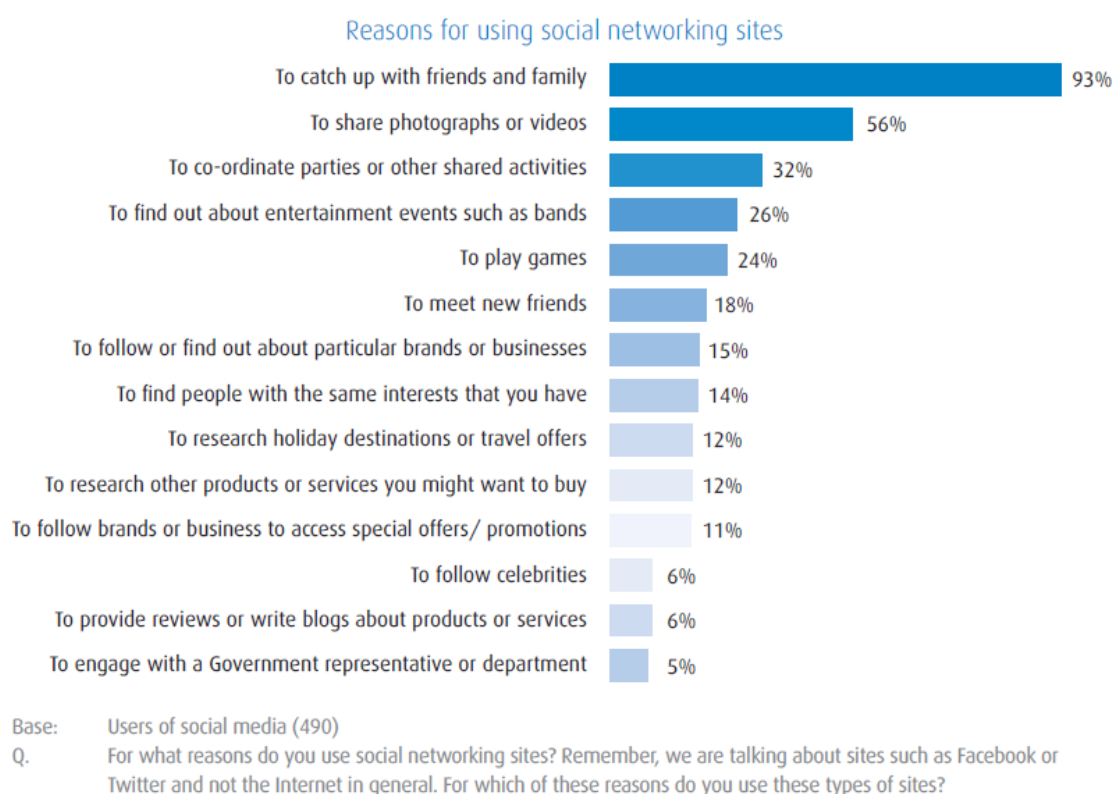


Figure 2.5: Reasons for using social media
(Source: Sensis 2011:18)

2.1.4 Trend: Emerging platforms

The trend towards increased use of social media has also meant a trend in emerging platforms, as technology businesses strive for a slice of the social media phenomenon. The most recent platform that has emerged is Google+ (Google plus). The timeline in Figure 2.6 provides some insight into the abundance of social network sites over the years. Most notably, the most popular social network site at the time of writing this report, Facebook, is the only one with a staggered release over time.

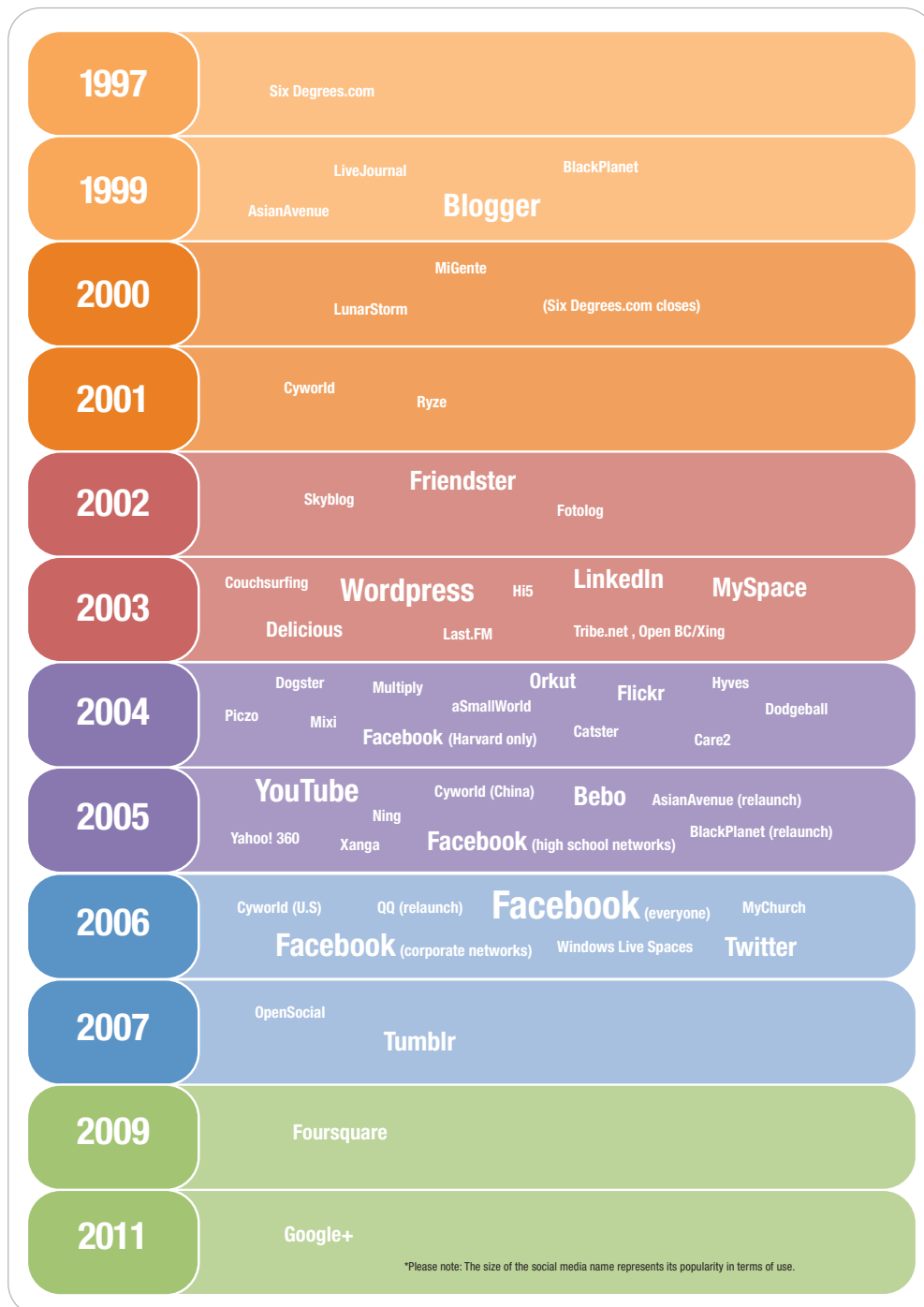


Figure 2.6: Timeline of social media platform releases (Source: Adapted from Boyd and Ellison 2008:212)

2.1.5 Trend: Facebook dominates

Facebook currently dominates social media use in Australia. It is the social media site with the highest recognition, highest number of users and highest frequency of use. The Sensis social media survey found that the average time spent on Facebook was 21.1 minutes on each occasion (Figure 2.7).

Time spent on social networking sites

Site	Proportion who use	Average time spent on each usage occasion						Average time (mins)
		Up to 2 minutes	3 to 5 minutes	6 to 10 minutes	11 to 15 minutes	16 to 30 minutes	Over 30 minutes	
Facebook	97%	5%	17%	22%	15%	19%	22%	21.1
LinkedIn	9%	19%	25%	10%	17%	16%	11%	13.1
Twitter	8%	29%	17%	22%	19%	8%	6%	11.4
Myspace	4%	28%	13%	19%	8%	13%	19%	14.8

Base: Users of social media (490)
Q. And roughly how long would you spend each time you use Facebook/LinkedIn/Twitter/MySpace?

Figure 2.7: Time spent on social networking sites
(Source: Sensis 2011:15)

The Sensis data also shows the frequency of use of Facebook among respondents; 18% said they used it more than 20 times a week, and the average use was 16.2 times per week (Figure 2.8).

Frequency of using social networking sites

Site	Proportion who use	Number of times per week						Average times per week
		Under 1	1 to 2	3 to 5	6 to 10	11 to 19	20+	
Facebook	97%	5%	20%	20%	24%	12%	18%	16.2
LinkedIn	9%	17%	31%	21%	14%	3%	14%	7.7
Twitter	8%	9%	15%	13%	28%	8%	28%	23
Myspace	4%	33%	46%	6%	14%	0%	1%	2.6

Base: Users of social media (490)
Q. In a typical week, how many times would you use Facebook/LinkedIn/Twitter/MySpace?

Figure 2.8: Frequency of use of social networking sites
(Source: Sensis 2011:14)

On average, people in the 14–19 year age group access social networking sites more than others, and people in Victoria have marginally higher Facebook usage.

The comparison of metropolitan and non-metropolitan groups shows that the more geographically distant from major areas/cities, the higher the usage of Facebook (Figure 2.9), which is possibly driven by a greater need for technology in order to keep in touch.

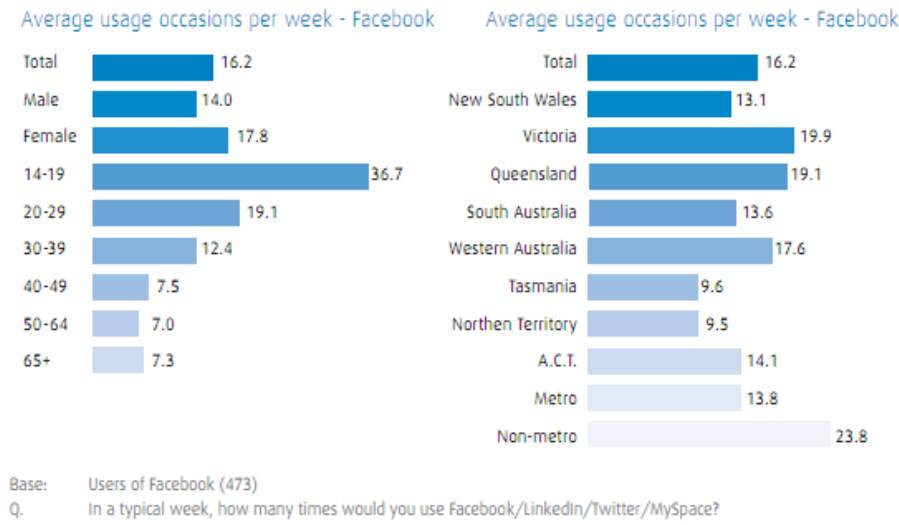


Figure 2.9: Average usage of Facebook (occasions per week)
(Source: Sensis 2011:14)

This review's public survey supports the Sensis data findings: younger people are the most frequent users of Facebook. Sixty-seven per cent of 18–24-year-olds access the site several times a day (Figure 2.10).

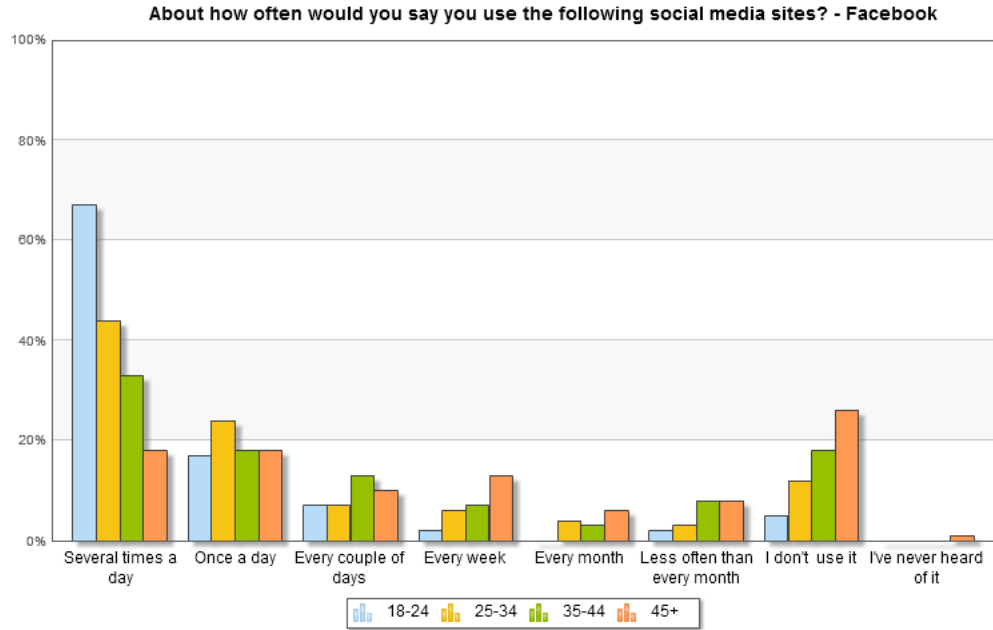


Figure 2.10: Use of social media by the general public

It is estimated that around 10 million Australians are on Facebook (Lee 2010). Facebook's own statistics in the Facebook advertising section support this estimate: at 21 July 2011, 10,436,860 people on Facebook stated that they lived in Australia (Facebook 2011). Facebook penetration, by state and territory, is shown in Figure 2.11.

Australian's on Facebook by State or Territory

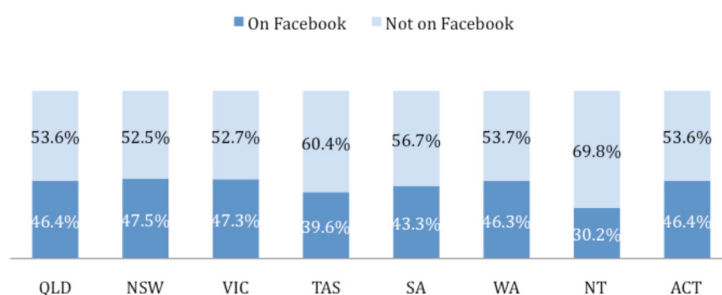


Figure 2.11: Australians on Facebook, by state and territory

(Source: adapted from Facebook 2011 and Australian Bureau of Statistics 2011)

It can be concluded from the above chart that the penetration by state suggests communication through Facebook may not be as effective for the Northern Territory as in New South Wales due to a lower percentage of the population with a Facebook account.

Facebook moves beyond Facebook

Facebook is also moving beyond its own site through the use of Facebook Connect, which allows Facebook's technology to be integrated into third-party web content. This enables Facebook likes, shares, recommends, and logins to be used across the web. Facebook is open to third-party developers via the Facebook API (application programming interface), which allows for access to Facebook databases, enabling thousands of applications to be developed (Facebook developers 2011).

At the start of 2010, Facebook connected itself to the wider web via a button labelled 'Facebook Like', which enables hundreds of millions of Facebook users across the globe to 'endorse' websites and web pages. The endorsements are automatically posted to users' Facebook walls. This created a massive infrastructure of interlinks between the 'social web' and what's been described as the 'searchable web' (Elowitz 2011). In June 2011, Facebook integrated into WordPress (an open source blog tool and publishing platform) through the WordPress Facebook and Twitter plugin, allowing people to use their Facebook accounts to login and leave comments on WordPress websites (Figure 2.12).

Leave a Reply

Enter your comment here...

☐ Notify me of follow-up comments via email.
 ☐ Notify me of new posts via email.

Figure 2.12: WordPress Facebook and Twitter plugin

(Source: Berkun 2011)

Facebook, the integrated social network

Sean Parker, one of the original investors in Facebook, was recently interviewed about why Facebook ultimately dominated Myspace. His insight is that Facebook grew organically from a niche market, then slowly went mainstream in a staged, geographically and, ultimately, dominating way (Tsotsis 2011).

Nobody actually believed, outside of us three or four people in Palo Alto, that you could enter the market through this niche market and then gradually, through this carefully calculated war against all the social networks, become the one social network to rule them all ,

- Sean Parker, Facebook investor
(Tsotsis 2011)

One reason why Facebook is 'sticky' (that is, able to attract users to return frequently) is that most users' social networks of 'friends' are in the one place, making it easy to communicate with them. Facebook captured the user interface, then went on to incorporate the best features of any social network (such as Twitter's 'What are you doing now?' and foursquare's geo-location check-ins). Possibly in response to Facebook's dominance of the digital social space, Google's new social network, Google+, contains similar features to Facebook, but with the inclusion of 'circles' to group friends. Circles have been better received than the Facebook lists (Solis 2011).

The success of Facebook may be attributed to its integrated nature: it includes elements of some other social media sites, amalgamating some of the key features into one social media platform (Figure 2.13). The Facebook platform is in a constant state of development and innovation, and new features are launched frequently, although their reception by Facebook users is often mixed.

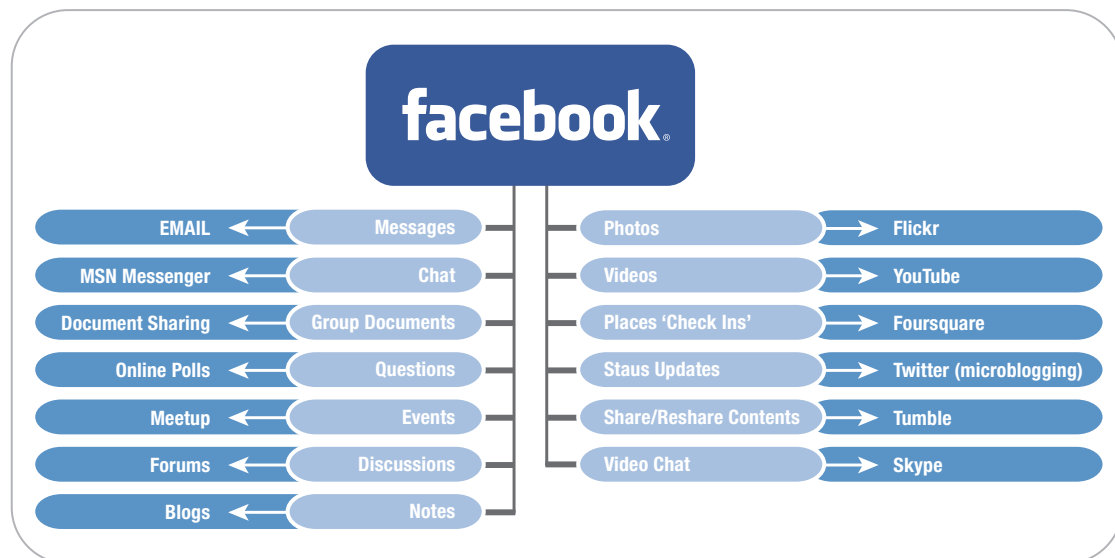


Figure 2.13: Facebook features that exist on other social media sites

2.1.6 Trend: Social media are mobile

Social media usage is increasingly carried out through portable or 'mobile' devices. Over the past 12 months, many Australians have upgraded to smartphones, and are moving away from standard text-and-call mobiles or web-enabled feature phones. Research by International Data Corporation indicates that the Apple iPhone leads the Australian smartphone market with 40% of market share in June 2011 (CNET Australia 2011). A 13% increase in iPhone shipments in the first quarter of 2011 puts the iPhone at nearly a third of the entire mobile phone market; Nokia's Symbian platform lost 9.5% of its market share (CNET Australia 2011).

Greater access to smartphone technology has helped Australians become more mobile in their social networking activities. In 2010, the most downloaded free iPhone 'app' (application) was the Facebook app (Gizmodo 2010). Mobile browser access to social networking sites is also rising. Global figures from January 2010 indicate that social networking access via mobile browser increased by 4.6% from the previous year, to 11.1% (comScore 2010). The tablet market is increasing: International Data Corporation forecasts strong growth in Australia and New Zealand in 2011 (CBR Communications Mobility 2011).

The Sensis social media report indicates that 34% of Australians surveyed used a smartphone to access their social media sites. The proportion was 52% for the 14–19 age group and 42% for 20–29-year-olds (Figure 2.13). This reflects the preference of the younger market, which increasingly has internet access most of the time.

Devices used to access social media

		Male (224)	Female (266)	14-19 (92)	20-29 (130)	30-39 (94)	40-49 (78)	50-64 (58)	65+ (38)
Desktop computer	60%	65%	57%	52%	52%	57%	66%	75%	81%
Laptop computer	50%	54%	62%	61%	70%	59%	54%	59%	24%
Smart Phone	34%	36%	31%	52%	42%	37%	23%	22%	0%
iPod Touch or similar	5%	3%	7%	10%	5%	4%	2%	7%	3%
iPad or other tablet	4%	1%	6%	2%	3%	5%	5%	8%	3%
Other	1%	0%	2%	2%	3%	0%	0%	0%	0%

Base: Users of social media (490)

Q. What devices do you use to access social network sites?

Figure 2.13: Devices used to access social media

(Source: Sensis 2011:17)

It was evident from this review's public survey that access to social media is mainly by a laptop or desktop computer, followed by mobile devices (Figure 2.14). For the purposes of this review, laptops were not considered to be mobile devices, as they are being overtaken by next generation devices specifically designed for mobile use and convenience.

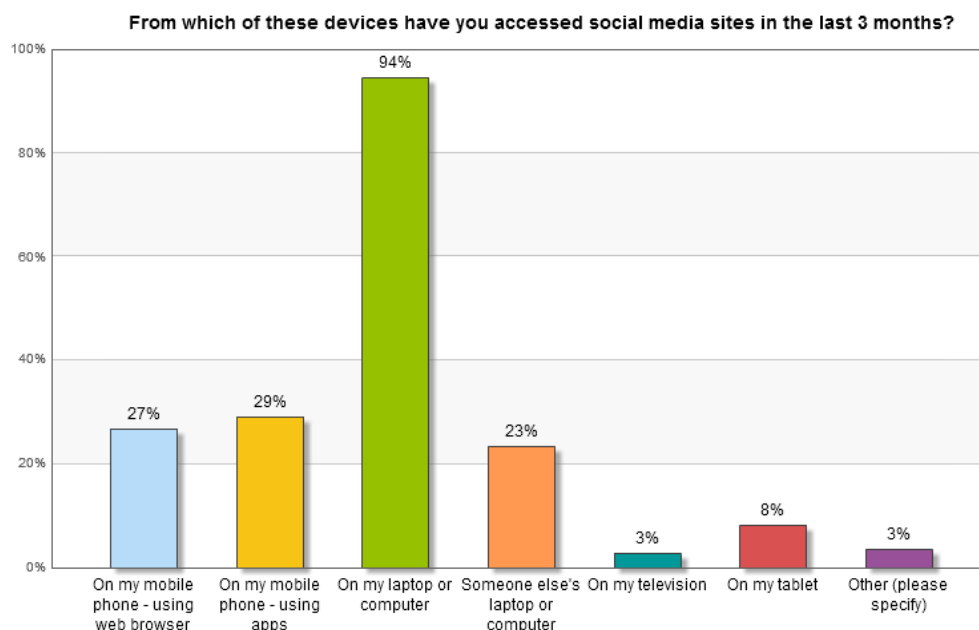


Figure 2.14: Devices used to access social media

The retail sector is being affected by social media users' ability to shop 'on the go'. Mobile shoppers are able to research purchase decisions, 'check in' (geographically), meet up with friends via 'People Nearby' on Facebook, and look for online deals, all while away from their main computer. Exploiting that mobility for marketing purposes is currently being trialled by foursquare through a partnership with 'daily deals' companies such as LivingSocial and Gily Groupe (Hutchings 2011). With the impending launch of QuickerFeet (an iPhone app for location-based promotions), this type of marketing may develop rapidly in the future (QuickerFeet 2011).

2.1.7 Trend: Social media integrate with technology

Social media are increasingly becoming integrated into daily routines and are being made easier to access through their integration into technology. There are two emerging methods for social media integration: pushing social networking sites on the public by forcing the sites into people's line of sight, and pulling people towards social media by creating exclusive content.

HTC mobile – the Facebook button



Given that social media mobile activity is on the rise (Net Marketing Strategies 2010), HTC has brought out a mobile phone with a Facebook button. This makes Facebook even easier to access than through the use of apps or web browsing. The button allows users to share information from their phone, such as photos, videos and messages, immediately. The phone also contains a Facebook chat widget, allowing users to connect with their Facebook friends who are online while on the go (HTC 2011). This is an example of Facebook being placed in the line of sight of the mobile phone owner or potential buyer. There is no option to remove the button or to make it inactive.

Mobile phone plans – free social networking

Tribe® is a social networking service that is FREE to Browse within Australia for Telstra Next G™ customers¹. It enables you to access and update Facebook®, Twitter™ and MySpace™ from a single location on your compatible Telstra Next G™ mobile.

With Tribe, you can:

- browse and comment on your friends' updates and photos
- view messages, wall posts and photo albums, and
- update your own status

all for FREE, while you're on the go.

You can also update your status and upload photos to one or more social networks simultaneously, saving you time.

Once you've added Facebook®, Twitter™ and MySpace™ to Tribe, there's no need to sign into each one separately anymore. Tribe is exclusive to Telstra and is available to most Next G™ Post-Paid and Pre-Paid customers with a compatible handset.

A number of phone companies now include free social networking as part of their mobile packages (Vodafone 2011). This is used to target heavier social media users, who would be wary about the amount of data usage on their phones when accessing social media. Telstra Tribe is a social platform that allows users to sign in to Facebook, Twitter and Myspace in the one place, free of charge (Telstra 2011). This type of social media technology integration can be seen as a push method, forcing social media onto the network user, as the Tribe platform cannot be removed from the phone plan.



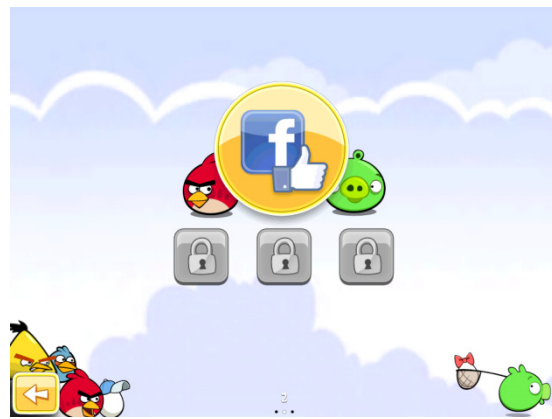
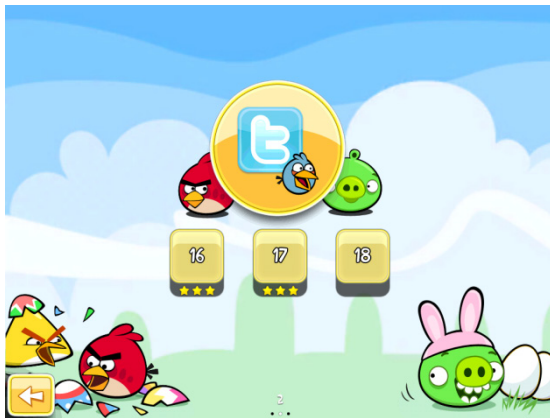
Unlimited social goodness for your mobile

We've made using your favourite social networks better.

We've done this by including free mobile access to Facebook®, Twitter, LinkedIn, FourSquare, and MySpace* in every new Vodafone mobile contract. And if you're on one of our older plans or caps, you can upgrade today to enjoy these great perks anywhere within Australia.

[Find out more](#)

Angry Birds – Facebook and Twitter to unlock levels



Facebook and Twitter accounts are required to unlock certain levels of the mobile game Angry Birds. This forces users to have a Facebook or Twitter account, or forgo the bonus levels (Games Blog 2011). This is an example of pulling the user towards social media by providing content that is available only to those connected to Facebook and Twitter. It is highly likely that this type of social media integration is designed to drive 'viral' awareness of the applications to 'friends' of the game's current user base.

2.1.8 Trend: Privacy is the new battleground

Different social networks provide different fields for information about users. Often, the more information provided, the higher the level of security and privacy required. Facebook asks for a person's first and last names, email address, birthday (for age verification purposes) and gender in order to create an account. Facebook also provides fields on a person's profile for friends and family, education and work, contact information and more (Figure 2.15).

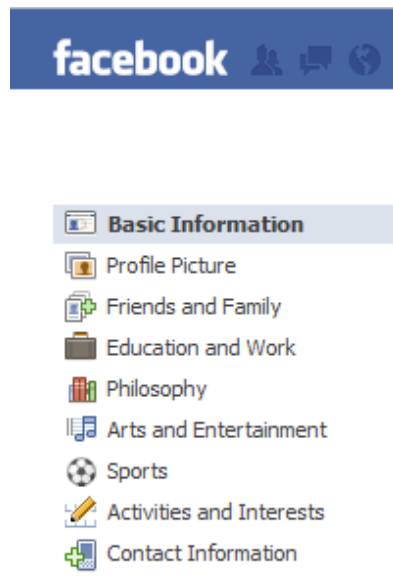


Figure 2.15: User information gathered on Facebook
(Source: Facebook, 18 July 2011)

Twitter, on the other hand, asks for only a name and an email address to sign up for an account and does not require that the account represents a real person, which is a requirement of Facebook. There are fewer opportunities on Twitter to provide information about a personal or organisational account holder, as the 'bio' (biography) section is limited to only 160 characters (Figure 2.16).

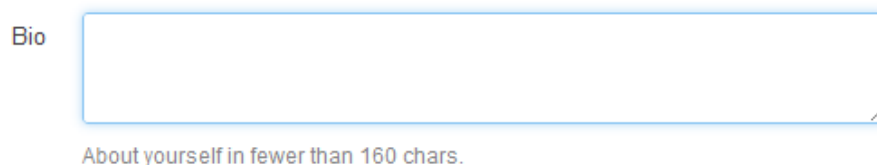


Figure 2.16: Bio section on Twitter
(Source: Twitter, 18 July 2011)

A number of social networking sites are similar to Twitter, requiring and providing for only limited information about the account holder. Others, such as Facebook, LinkedIn, Myspace and Google+, require and provide fields for detailed information about the account holder. This is why users have higher privacy expectations on some social media sites than they might on others.

To an extent, Facebook changes its privacy settings to fit the requirements of the community, although some information must remain available to the public eye. Because many types of personal information can be uploaded onto Facebook, the privacy settings are more complex than those of some other social networking sites. Interestingly, Facebook uses an ‘opt out’ approach for any new features to the site, such as Facebook Places and automatic photo-tagging. With Facebook Places, users can be ‘tagged’ by friends at certain locations without their permission, showing their exact geographical location to all of their Facebook friends and the friends of the person who tagged them. To opt out and ensure that their location is not disclosed by friends, users must go to their Facebook privacy settings and disable the feature.

Automatic photo-tagging on Facebook was released in Australia in early June 2011 but suffered negative backlash from the public, prompted by a blog post by Graham Cluley of the security firm Sophos, criticising the opt-out nature of the feature (ABC 2011). The feature prompted an investigation by European Union data-protection regulators as a potential privacy risk, the concern being that the opt-out process means users have not specifically consented (Schroeder 2011). Of the respondents to this review’s public survey, 46% did not know whether automatic photo-tagging was enabled on their account. Facebook often puts the onus of privacy and security of information on the account holder.

This review’s public survey asked participants when they had last reviewed or altered their privacy settings on Facebook (Figure 2.17). Nine per cent indicated that they did not know how to review or alter their settings.

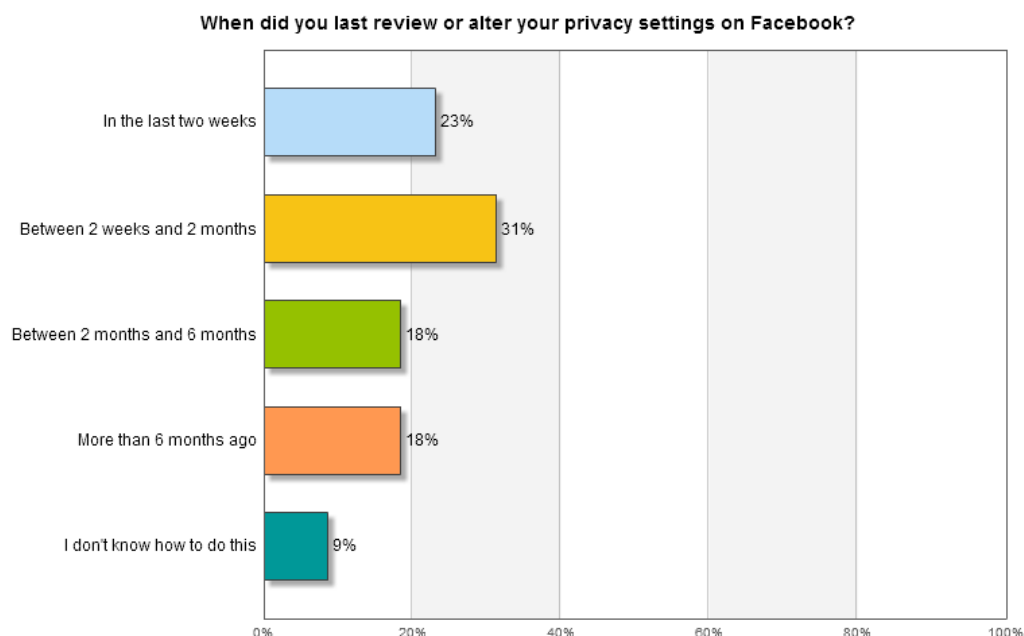


Figure 2.17: Facebook users’ alteration of privacy settings

Most respondents indicated that their Facebook profile settings are generally set to friends only, although 5% had most of their information viewable by the public.

2.1.9 Trend: Social media alter news reporting

Social media are increasingly becoming methods for journalists to collect and communicate information. Most Australian news networks have a presence on social media, primarily on Twitter. Realtime updating means that news companies are able to break stories as soon as they happen. Online news sites, newspapers, TV news and radio are using social media both to get their messages out and to be the first to market with information. Individual journalists are also using social platforms such as Twitter to communicate news (Figure 2.18).

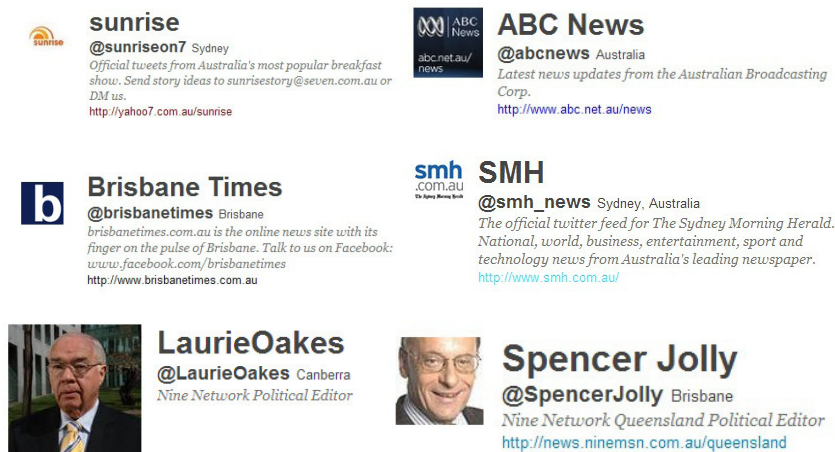


Figure 2.18: Twitter accounts of news organisations and individual journalists

(Source: Twitter, 20 July 2011)

Social media have become so important to journalists and news companies that they have prompted the development of guidelines and education for journalists using them to report news. For example, Reuters (2011) has produced a guide called 'Reporting from the internet and using social media' (Figure 2.19).

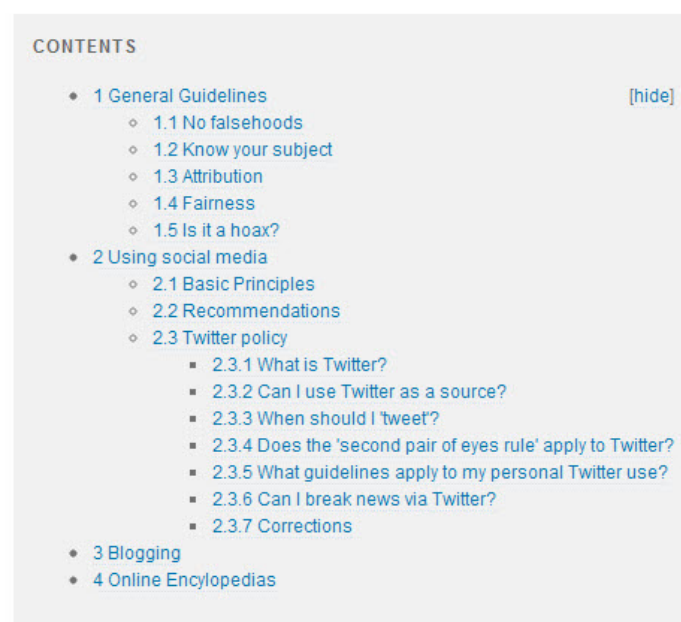


Figure 2.19: Guide to social media use for journalists

(Source: Reuters 2011)

One of the most interesting sections of the Reuters guide is '1.5 Is it a hoax?'. Hoaxes have been a problem for some journalists who have failed to verify facts found in social media before broadcasting the story, either in social media or through traditional media channels (Mashable 2011).

'Jeff Goldblum dead'

In 2009, an entertainment reporter took from Twitter the assertion that actor Jeff Goldblum had died in an accident in New Zealand, and reported it on a morning news show. The report claimed that the New Zealand police had confirmed the death of Goldblum after he had fallen from a cliff during a film shoot. However, Goldblum was alive and well (Daily Telegraph 2009). It took an email from a viewer to prompt the TV show to dismiss the story as a hoax (Newsphobia 2009).

'Queensland floods – crocodile in Gympie'

The 2011 Queensland floods were covered extensively by news reporters. Local authorities' tweets about the floods, safety, evacuation and road closures, and Premier Anna Bligh's Twitter account, became important sources of information. On 11 January 2011, an image surfaced on Twitter allegedly showing a crocodile brought into Gympie by the floodwater (Figure 2.20). The image received more than 30, 000 views and was featured in the main news flood coverage, including television news. The image was a hoax: it had been adapted from a commercial.

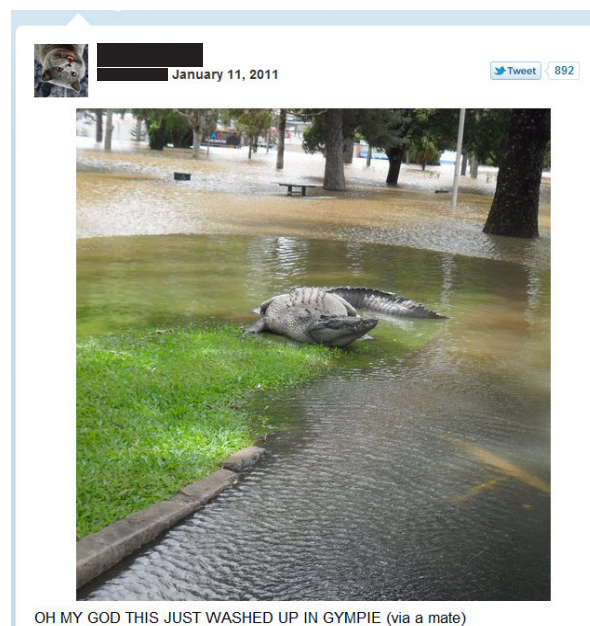


Figure 2.20: Twitter post during Queensland floods
(Source: Twitpic 2011)

Social media is changing news reporting forever, by giving journalists and news networks a new platform to communicate to many people, with real-time updates. Speedy supply of information is important for journalists, but it must be noted that the use of social media for information-gathering does have its pitfalls and can result in false information being further dispersed, if it is not verified prior to re-broadcast.

2.2 LEGAL OBLIGATIONS



The following has been prepared for the review by Stephen von Muenster, Principal, von Muenster Solicitors & Attorneys.

Stephen von Muenster
Principal von Muenster Solicitors & Attorneys

Overview

Forming part of the George Patterson Y&R, Department of Defence (Defence) Social Media Review Scope of Work, this brief overview is divided into nine sections and is designed to examine the laws that may influence and restrict Defence participation and engagement in social media. This review is a high level examination and is primarily aimed at Defence and its members' engagement with a broad internal and external community of organisations and individuals that are interested in the activities of Defence.

Firstly, we introduce the concept of social media and explore the notion of user-generated content. What this overview understands to be participation and engagement in social media by Defence and its members is then placed into context through a classification of professional use and private use of social media.

We then examine the laws that have the potential to impact upon such professional and private use. Given the time available to prepare this overview, specific defence and public service legislation, including freedom of information, public records management and archiving requirements, are not considered in detail and are beyond the scope of this brief overview. The same applies to extant defence policies and guidelines, including for example equity & diversity and information & operational security. The specific application of such legislation and policies are best examined and will need to be considered further once Defence has indicated how it intends to embrace and engage in social media as an organisation following consideration of the preliminary George Patterson Y&R Social Media Review.

Finally, we suggest a holistic risk management based approach to legal compliance in social media engagement. Such an approach is necessary as there is no specific law in Australia governing social media – the current state of the law is evolving, uncertain and remains largely untested in the Courts – and the application of the complex coalition of laws and private contracts that do apply are generally misunderstood in the social media space. The reality that social media engagement results in instantaneous global communication resulting in the possibility of attracting the jurisdiction of current and emerging overseas laws and regulations unfortunately adds to this complexity.

Our legal overview concludes with some suggested practical approaches and risk treatment strategies when Defence and its members engage in social media (termed ‘Social Media Policies’) and when Defence allows third parties to engage with the Defence through an exchange of user-generated content (termed ‘Engagement Principles’). It is suggested that such an approach will go a long way to increasing confidence in the use of social media whilst removing uncertainty and reducing the likelihood of the occurrence of identified and unidentified legal and reputational risks in social media engagement.

The sections of this overview are as follows:

Introduction

Social Media Engagement in Context

User-generated Content

Regulation of Social Content

- Introduction
- Internet Content Regulation

Laws Influencing and Restricting Defence Engagement in Social Media

- Introduction
- Who might complain?
- International laws that may apply to social media engagement
- Consumer protection laws
- Passing off
- Trade marks
- Copyright
- Moral rights
- Defamation
- Discrimination, hate speech & causing offence
- Injurious falsehood
- Privacy laws
- SPAM laws

The Rules of Proprietary Space

Social Media Engagement Principles

Social Media Policies

Closing Observations

Introduction

We are in the midst of a social media revolution. Social media is a revolution in the way in which individuals, consumers, government, business, non-government organisations and the media engage and communicate with each other.

Social media is often understood to describe media or content that is authored or generated by a user and can take numerous forms. Social media includes forums, bulletin / message boards, blogs, wikis, podcasts, posts, threads. Social media sites or applications such as Google, Facebook, LinkedIn, Twitter and YouTube provide a social networking environment enabling community engagement and interaction between individuals and groups.

Social networking sites continue to evolve as integrated hubs for entertainment, information and communication. Social sites are becoming increasingly integrated. Blogs, posts, tweets and videos created by users and their friends can be broadcast simultaneously for example on Facebook, LinkedIn, Twitter and YouTube. As individuals, consumers, government, business, non-government organisations and the media are dynamically engaging in social media, it has become the new reality that the reputation of organisations or individuals can be harmed or enhanced through the socialisation of good and bad experiences on social networking and social media sites.

Openness is a feature of internet technology and such openness underpins its original architecture, software development and open access. Given this foundation, it must be understood that engagement in social media necessarily involves an organisation relinquishing some control. In the past, organisations were able to determine the relationship with its members or the public. Thanks to social media, it is the members and other individuals who increasingly are defining how an organisation is perceived. Instead of being simply passive receivers of information, individuals of today are actively engaged and are participants in a conversation with the organisation. Rather than trying to remain in control, organisations must embrace the opportunity whilst adopting an altered set of internal policies and external engagement principles that ensure compliance with the current and emerging legal obligations that apply in social media. Such an approach will go a long way to reducing legal and reputational risk.

The aim of this review is to provide Defence with a highlights tour of the Australian laws and regulations that may, on a case by case basis, influence and restrict Defence participation and engagement in social media. This overview does not attempt a comprehensive or 'deep dive' review of each of the applicable laws as such an examination is presently beyond the George Patterson Y&R Scope of Work. Furthermore, this legal overview does not examine the complex art of social media marketing and consumer engagement, as such an enquiry is best left to the experts.

Instead the intent of this overview is to raise the general level of awareness of the applicable laws and regulations as well as identify some of the risks inherent in social media engagement. In turn this may promote legal compliance and thereby reduce legal and reputational risks to Defence and its members when engaging in social media.

Finally, as each social media channel and communication is different and raises its own legal and compliance challenges, it would be impossible for this overview to provide specific legal advice. Therefore it is important to understand that this overview is intended as a guide only and should not be relied upon in substitution for seeking appropriate legal advice on a case by case basis.

Social media engagement in context

Use of social media and the procedures and policies designed to regulate the manner of its use will be largely be dependent on the nature and interests of a given organisation, the type of community that may engage with the organisation and the practices and needs of its members. There is no standard or 'one-size fits all' approach.

For the purposes of examining the Australian laws that may influence and restrict Defence participation and engagement in social media, we have considered it necessary to take a broad view of the types of Social Media use that may involve Defence and its members. The following possible scenarios involving Defence and its members are considered:

The following nature of use referred to in this overview as **Professional Use**:

- Defence as an organisation maintaining its own socially enabled website and having an active presence via pages on the social media sites or applications. Examples include the Army internet site and Army Facebook, Flickr, Twitter and YouTube pages.
- Defence engaging in various mainstream and niche social media channels via participation and conversations on other social media sites, the pages or channels of other organisations or the media and forums, bulletin / message boards, blogs, wikis, podcasts, posts, threads and the like.

The following nature of use referred to in this overview as **Private Use**:

- Defence members with their own active presence on the social media sites and participation in the mainstream and niche social media channels where members refer to their involvement with or employment by Defence in any way, including identifying themselves as Defence members, discussing their activities and the activities of other Defence members and posting user-generated content related to their Defence activities.
- Defence members engaging and participating in social media without any reference to Defence; although the Defence member may be known

in his or her community to be a Defence member, or an association with Defence may be inferred.

The Australian laws and regulations discussed in this overview may apply in varying degrees to the type of engagement in social media identified in each of the above scenarios. Further, the distinction between Professional Use and Private Use is very important when considering the content of a Defence Social Media Policy (discussed in greater detail below).

User-Generated content

Engaging in social media is all about sharing and collaboration. Social media involves a conversation – a ubiquitous, borderless, worldwide multi-way conversation with potentially an unlimited number of individuals conducted through a combination of written, visual and aural material. The result is the generation of user-generated content by the individual or organisation who engages in social media.

Today individuals are experimenting with and creating user-generated content. Empowered individuals modify, edit and change existing content as well as create a wide variety of their own material through the combined effect of personal computers, digital cameras, digital video recorders, technology rich mobile devices, the internet, enabling software and the various formats offered by purpose created websites. User-generated content includes combinations of written posts and comments, data, text, software, speech, music, sounds, visual images, photos, video (animated or otherwise), and other creations and combinations generated by an individual.

File sharing and social media sites are available to any individual with an internet connection enabling them to instantaneously upload and post their social content creations to share with their online communities. Individuals are also creating new types of content by incorporating their own material with commercially created film, music and other content (sometimes referred to as ‘mashups’). This is often done without any regard for copyright laws (discussed further below).

For Defence and its members such user-generated content will be generated as a result of both Professional Use and Private Use. As engagement in social media and the creation of user-generated content are inextricably linked, Defence must establish community requirements or engagement principles for user-generated content submissions that prohibit infringing and offensive content. Defence Social Media Policies for Professional Use and Private Use (discussed below) regulating and suggesting appropriate creation of user-generated content by Defence members and Engagement Principles applicable

to third parties' engagement with Defence (also discussed below) will assist with legal compliance and significantly reduce the risks of engagement in social media.

Regulation of Social Content

Introduction

Content laws to refer to the coalition of Australian laws, regulations, determinations, standards and industry codes that directly impact upon the nature and type of **content** (written posts and comments, images, photos, video and other creations and combinations) that can lawfully be seen, heard, communicated, broadcast, streamed or downloaded via social media.

Content laws can apply equally to repurposed traditional content, premium content, advertising content, branded content and even to user-generated content. Therefore if Defence itself creates content or invites user-generated content during Professional Use, Defence will need to consider the application of content laws on a case by case basis. The content laws also apply to Private Use.

In Australia, the Australian Communications and Media Authority (ACMA) is responsible for regulating the nature and type of content that may be published online including internet and mobile social content, and enforcing Australia's anti-spam law. Content is primarily regulated through a number of Commonwealth laws, regulatory standards determined by ACMA, and industry initiated mandatory and voluntary industry codes of practice.

There are numerous regulatory standards and codes that apply to the broadcasting, telecommunications, radiocommunications and internet industries and it is beyond the scope of this overview to provide a review. In this section we only seek to overview the regulation of social content to the extent that such regulation is likely to impact upon Professional Use and Private Use in social media.

Internet Content Regulation

ACMA administers a national co-regulatory scheme for internet content which is governed by the **Broadcasting Services Act 1992**, and is designed to address community concerns about offensive and illegal material on the internet. A regulation of content framework came with the introduction of Schedule 7 to the **Broadcasting Services Act 1992** which commenced on 20 January 2008.

Internet content is regulated under the national co-regulatory 'Online Content Scheme'. The internet content regulations apply to all hosting, content and links service providers, and providers of live (streamed) content from Australia. This generally means any person

or organisation that makes internet content available, but not producers of internet content or persons who uploaded or accessed internet content.

Internet Content is defined in Schedule 5 of the **Broadcasting Services Act 1992** as information that is kept on a data storage device and is accessed or available for access through an internet carriage service (a service that enables end users to access the internet). This includes websites, usenet newsgroups, peer-to-peer file sharing applications, live content such as 'live' streaming audio / video and adult chat services, and other types of content that can be accessed online or on a mobile phone, but does not include email.

Under the **Broadcasting Services Act 1992**, the following categories of internet content are prohibited:

Any online content that is classified RC (Refused Classification) or X 18+ by the Classification Board (formerly the Office of Film and Literature Classification). This includes real depictions of actual sexual activity, child pornography, depictions of bestiality, material containing excessive violence or sexual violence, detailed instruction in crime, violence or drug use, and/or material that advocates the doing of a terrorist act.

Content which is classified R 18+ and not subject to a **restricted access system** that prevents access by children. This includes depictions of simulated sexual activity, material containing strong, realistic violence and other material dealing with intense adult themes.

Content which is classified MA 15+, provided by a mobile premium service or a service that provides audio or video content upon payment of a fee and which is not subject to a **restricted access system**. This includes material containing strong depictions of nudity, implied sexual activity, drug use or violence, very frequent or very strong coarse language, and other material that is strong in impact.

Classifications are based on criteria outlined in the **Classification (Publications, Films and Computer Games) Act 1995**, **National Classification Code** and the **Guidelines for the Classification of Films and Computer Games 2005**.

If the content is hosted in or provided from Australia and is prohibited, or is likely to be prohibited, ACMA will direct the content service provider to remove or prevent access to the content on their service.

If the content is not hosted in or provided from Australia and is prohibited, or is likely to be prohibited, ACMA will notify the content to the suppliers of approved filters in accordance with the Internet Industry Association's Codes of Practice.

If the content is also sufficiently serious, for example, illegal material such as child pornography, ACMA may refer the material to the appropriate law enforcement agency.

Laws Influencing and Restricting Defence Engagement in Social Media

Introduction

In this section of the overview, we will examine the legality of the **information, claims, messages** and **elements** contained within social media communications.

There exists a coalition of Australian laws and regulations that can influence and restrict **claims, messages** and desired **take outs** – achieved via a combination of content including moving and still images, text, logos, music and voice - contained within social media communications.

The laws that apply to communications upon conventional media also apply to social media communications. However, Defence and its members, when using social media for Professional Use and Private Use, face challenges in seeking to apply the existing laws to their communications due to the unique and evolving nature of social media.

As the social space is still being defined, any attempt to lay down a precise formula or code for Defence to follow on how to apply the existing laws to social media risks becoming obsolete by the time this overview is reviewed. Social media technology, platforms, applications, sites and communications techniques are simply evolving too rapidly.

Instead, in this section of the overview, we provide a **social media flavoured** overview of the relevant laws that exist today together with impending areas of law reform for Defence to bear in mind as it plans and executes social media campaigns and for Defence members to have regard to when they engage in social media.

Who might complain?

Social media communications are likely to impact upon a diverse range of interests and not all will be charmed by the social media message. There are numerous organisations, businesses and individuals that may feel aggrieved by the communication and who may wish to seek some form of legal or quasi-legal remedy to challenge the campaign or engagement, for instance:

- consumers who are misled or deceived by the message or are simply displeased by what they see;
- competitors who see their market share under threat;
- celebrities, character or brand owners whose ability to profit from endorsement may be diminished by an unauthorised use of their image, character or brand;
- community interest groups who may be particularly enraged by the message;
- individuals who may have their reputation and character brought into question by the message;

individuals who may claim that their privacy has been unfairly compromised;
artists, musicians or writers whose original work may appear in the communication without their knowledge or consent; and
Government bodies such as the ACCC who monitor communications and protect consumers.

To avoid costly court proceedings, adverse publicity or even the expense of discontinuing or modifying a campaign, any social media engagement that Defence intends to conduct should be cleared by Defence Legal or an external experienced legal professional to ensure compliance with the laws outlined in this overview that may impact upon the engagement.

International laws that may apply to social media engagement

Before launching into an overview of the laws that might apply to a proposed campaign or engagement, it is perhaps worth stating the obvious by noting that the internet and other digital technologies have brought about dramatic changes in the way individuals interact. Business can now be transacted all over world, transcending distance, time, borders and nationality. This is the realm of cyberspace.

Accordingly, a particular Australian campaign or engagement conducted via the social media channels or other digital technology has the distinct possibility of attracting 'global liability' where Defence or its members could potentially be subject to the laws of any country or state in the world. Still very much evolving are worldwide legal principles that determine whether a given country's laws apply to a given site or communication originating in another part of the world, but viewable and able to be interacted with within a different country.

Defence must be alive to the possibility that use of the internet and social channels for a campaign or engagement intended for Australia, may not only attract individuals in another part of the world but might also result in organisations, businesses or individuals feeling aggrieved by the communication and therefore the risk of the application of foreign laws and regulations.

Evolving Australian and worldwide laws tell us that there are steps that can be taken to reduce the risk of global liability:

Subject to specific legal advice to the contrary, take the initial view that if the website or other social media can be accessed by individuals in a given country, then that country's laws may apply to the media, the content of the communication and the message. If Defence or a Defence member is breaching one of the applicable Australian laws outlined in this overview, it is quite possible that an equivalent law will be breached in the overseas country.

To avoid being taken to court in the USA (and possibly in an increasing number of other countries), Australian websites need to ensure they do not create a campaign that somehow 'targets' the USA generally or one of its States, cities, geographical or cultural icons or persons resident. However, passive communication by itself is usually not sufficient to attract the reach of USA courts.

Consider prominent notices or country and state disclaimers about the reach and target of the site or page – what countries it is intended for and limitations based on nationality, language, currency or post code.

Consider limiting the nationality of the people that can actually access a website or alternatively, subscribe to online services available via the website.

Consider including appropriate choice of law and choice for forum (place for determination of disputes) conditions in the Engagement Principles that must be agreed to in advance.

Consider using appropriate IP address blocking technology.

Consumer protection laws

The **Australian Consumer Law (ACL)** contained within Schedule 2 to the **Competition and Consumer Act 2010 (Commonwealth)** is now the preeminent piece of legislation that protects consumers against false communication and promotion.

The ACL applies as a law of the Commonwealth under the **Competition and Consumer Act 2010** and as a law of each Australian State and Territory by virtue of separate application legislation. As a result there is now one uniform consumer law throughout all jurisdictions in Australia.

Under the former **Trade Practices Act 1974**, the consumer protection provisions applied to corporations only. The equivalent provisions in the ACL are now directed to the conduct of 'persons', which include corporations, a body politic and individuals. Under Section 2A of the **Competition and Consumer Act 2010**, it is clear that, in so far as they carry on business, the Commonwealth and Commonwealth authorities are subject to the act.

A detailed examination of whether future engagement by Defence in social media has the potential to be caught by the **Competition and Consumer Act 2010** is beyond the scope of this overview. However, it is sufficient for our purposes to observe that provided the conduct has a sufficient trading and commercial character and a nexus with trade and commerce, there always exists the possibility that Professional Use and Private Use of social media may be caught by the ACL.

Adopting policies, practices and engagement principles in social media that are designed to comply with the ACL will go a long way to reducing the legal, commercial and reputational risks that may arise in social media.

The following are the primary consumer protection Sections of the ACL that may impact upon social media engagement and of which Defence and its members should be mindful:

Section 18 prohibits conduct that is misleading or deceptive or is likely to mislead or deceive. The remedies for a breach of Section 18 include injunctions, damages and corrective advertising.

Section 29 prohibits false or misleading representations, for example, false claims as to association, sponsorship, approval or affiliation, false claims as to price, false claims as to standard, quality, value or grade, false claims as to whether a product is 'new' or false testimonials. A breach of Section 29 may attract criminal penalties under Chapter 4 of the ACL, such as fines.

Section 48 'Clarity in Pricing' provides that promoters must ensure 'all-inclusive' pricing in consumer campaigns. In order to prevent the creation of an impression that a product is being offered for a sale at a lower price than it actually is, advertising must prominently feature, as one price, the total amount a consumer must pay. That price must include all mandatory charges, taxes, duties, levies and all amounts payable under law. In other words, any cost that can be assigned a dollar value must be included in that one price. However, if elements of the price cannot be determined ahead of time or will vary depending upon the customer's choice (i.e. they cannot be 'quantified' or will genuinely vary) those elements do not need to be included in the single price. In such cases it would be acceptable to state a 'from' price, provided of course that the price stated is accurate and it is clear that other price elements will depend on certain disclosed consumer choice or location factors (for example).

Section 32 states that it is illegal when promoting products to offer rebates, gifts, prizes or other free items with the intention of not providing them, or of not providing them as offered. A breach of Section 32 may also attract criminal penalties under Chapter 4 of the ACL.

Section 35 renders the practice of 'bait advertising' illegal. A breach of Section 35 may also attract criminal penalties under Chapter 4 of the ACL.

Section 49 prohibits businesses representing to consumers that they will receive a rebate on the agreed price of products or some other benefit in exchange for the names of other prospective customers if the receipt of the rebate or benefit is conditional upon a future event occurring. A breach of Section 49 may also attract criminal penalties under Chapter 4 of the ACL.

Section 18 Australian Consumer Law – Misleading or Deceptive Conduct

Section 52 of the former **Trade Practices Act** was one of the most litigated provisions existing in any Australian law. Section 18 of the ACL is in identical terms and the body of decided case law applying to Section 52 now applies to Section 18.

Section 18 is likely to be used by the organisations, businesses and individuals identified above if they feel sufficiently aggrieved by a social media engagement so as to commence legal proceedings.

To 'mislead or deceive' means to lead into error. This means that to infringe Section 18 the message in the social media communication would usually contain some form of misrepresentation. A message that merely causes a person to wonder or be somewhat

confused or uncertain will not usually be misleading or deceptive. People are accustomed to ‘puffing’.

In the social media communications context, a misrepresentation giving rise to breach of Section 18 can be caused or conveyed by one or a combination of written words, spoken words, images, graphics, video, animations, action sequences, music and silence.

It will be important for Defence during Professional Use of social media to objectively scrutinise any proposed communication or received communications from third parties for claims and representations that may be misleading or deceptive to the target audience.

Determining where to draw the line as to what is misleading or deceptive and what is not can be notoriously difficult in the social media communications context. There will of course be conduct and claims that are clearly deceptive in a given circumstance and conduct and claims that are clearly not. It is the edgy social media engagement mechanics and messages designed to draw people in that highlight the positives and understate the limitations that ‘sail close to the wind’ from a consumer protection perspective.

Examples of a Section 18 breach in Social Media

Comments by Third Parties on Facebook and Twitter pages: **ACCC v Allergy Pathway Pty Ltd [2009] FCA 960**

Allergy Pathway operates clinics for the diagnosis and treatment of allergies. In early 2009 the ACCC commenced proceedings against Allergy Pathway in respect of representations concerning its allergy diagnosis and treatment services. The representations were made in a series of publications. At the hearing Allergy Pathway did not contest the ACCC’s allegations and the court found that it had engaged in misleading and deceptive conduct in contravention of the then Section 52 of the **Trade Practices Act 1974**. Undertakings were given that the same or similar representations would not be made again for a period of three years.

Subsequently, the ACCC became aware that Allergy Pathway had continued to make representations concerning its services that were in breach of the undertakings given. The representations were found to have occurred in social media via the following channels:

- statements and links to statements posted by Allergy Pathway on its website, Facebook and Twitter pages and in a video posted on YouTube and on its Facebook and Twitter pages;

- testimonials written by Allergy Pathway’s customers and posted by Allergy Pathway on its website, Facebook and Twitter pages;

- Allergy Pathway’s responses to queries posted by members of the public on its Facebook ‘wall’; and

- testimonials written and posted by Allergy Pathway’s customers on its Facebook ‘wall’ – in this instance Allergy Pathway was found liable for the postings of third parties on Facebook because it knew that misleading testimonials had been posted on Facebook and Twitter and it took no steps to have them removed.

The significance of this decision is that organisations that promote themselves via social media channels including Facebook, YouTube and Twitter are now responsible for monitoring the content of their social networking sites and in particular user-generated content that is posted by third parties. If such content is misleading or deceptive, it should be removed.

Fake Profiles: Australian Competition and Consumer Commission v Jetplace Pty Ltd [2010] FCA 759

Jetplace operates an adult social networking and dating site known as ‘redhotpie’ that is used for social, dating and entertainment purposes. Members of the website create individual user profiles describing their characteristics and exchange ‘flirts’ and customised messages with other members.

The directors of Jetplace developed and implemented a formal policy at Jetplace surrounding the creation of fake profiles that were programmed to automate and schedule the sending of flirts and other messages to members and to appear in the visitor history of member profiles. Despite the creation of more than 1300 fake profiles, Jetplace represented on its website that:

- every profile had been created by a visitor to the site;
- any profile identified in a member’s search was created by another member; and
- every message received from a profile provided an opportunity to socialise on the website and potentially meet with another member.

The Federal Court found this conduct to be misleading and deceptive and that the website contained false and misleading representations. The site had to undertake corrective advertising by telling each user of the deceptive conduct when they logged on and also by sending a copy of a court imposed notice to the email address of each user.

This decision is important as it confirms that organisations must not mislead or deceive individuals during the process of social media engagement. For instance, organisations

would not be able to create false comments or posts to their site or Facebook page that purport to be from individuals when in reality they were created by the owner of the site or page. The same would apply to the uploading of fake user-generated content by the site or page owner that purports to be from a genuine third party who has an interest in the organisation.

Passing off

The old passing off tort action under the common law is different from the consumer protection laws discussed above and instead is designed to prevent a trader from damaging another trader's reputation or goodwill by causing potential consumers to associate one trader's product or business with another trader's where no such association exists.

The passing off action can be used to protect brand and business names as well as a product's 'get up' and even a distinctive social media campaign. The passing off action can be used by one trader against another, if:

- the innocent trader's get-up, including the brand name or business name is recognised by consumers as having a distinct and established reputation;

- there has been a misrepresentation by the offending trader to consumers leading consumers to believe that the products offered by the offending trader are in fact the innocent trader's products; and

- the innocent trader has suffered or is likely to suffer damage to its business by reason of the erroneous belief created by the offending trader's misrepresentation that the source of the offending trader's products is the same as the source of those offered by the innocent trader.

Organisations need to bear the passing off action in mind when developing social media campaigns, particularly when the intended product to be promoted directly competes with another established brand or utilises the reputation of a well known brand or personality and the intention is to piggy back or cash in to a certain degree upon the established brand's or personality's identity and reputation.

For example, the tort of passing off and breach of the Trade Practices Act was used by Lara Bingle in a 2006 Federal Court action against a men's magazine which published topless photos of her without her consent or permission. Similarly, the uploading of content by individuals and organisations to social media sites or pages in the form of images of well known celebrities or brands may result in a passing off action if there is a sufficient commercial nexus and the elements of passing off can be established.

Trade marks

Trade mark law in Australia is governed by the **Trade Marks Act 1995 (Commonwealth)**. By virtue of Section 3, the Trade Marks Act applies to the Crown in the right of the Commonwealth.

A trade mark is any **sign** used to distinguish goods or services of one trader from those of

another. A sign includes a letter, word, name, signature, numeral, device, brand, heading, label, ticket, aspect of packaging, shape, colour, sound or scent.

Trade marks are a vital tool in the brand protection arsenal. Most are familiar with Apple's registered trade mark 'iPod' and other 'Pod' or 'i' related branding and Apple's battle to stop other organisations laying claim to 'pod' and to prevent 'pod' falling into general usage.

It is also possible for phrases and slogans to be registered as trade marks, and for trade marks to play a significant role in the legal protection of celebrity personality in Australia. Increasingly, celebrities are turning to the protection offered by trade mark registration to prevent the unauthorised exploitation of their personalities in the commercial realm. Trade mark registration can protect various indicia of celebrity personality such as their name, signature and likeness.

When a trade mark is registered with the Trade Marks Office, it is registered in either one or more particular classes of goods or services that closely relate to the business that the proposed trade mark will promote in the marketplace. There are 45 different classifications of goods and services pursuant to which trade marks may be registered.

A trade mark owner has, subject to certain exceptions, the exclusive right to use and apply the trade mark to particular goods and services and to authorise other persons to use the trade mark by way of a licence.

Trade mark infringement can occur if an individual or organisation, without the consent of the trade mark owner (for instance without a licence deal), uses in social media communications a '**substantially identical**' or '**deceptively similar**' sign as a trade mark (i.e. used to indicate the origin or source of the products), in one of three ways:

- in relation to the goods and services in respect of which the mark is registered;
- in relation to goods or services which are the 'same as' or 'closely related to' the goods or services for which the mark is registered; or
- in relation to 'unrelated' goods or services, if the registered mark is well known or iconic in Australia and if the use is likely to suggest a trade connection with the trade mark owner.

Protection is absolute in the sense that that once wrongful use of the trade mark has been established by the trade mark owner, infringement is proven and there is no need to prove that there is confusion in the marketplace or damage as is the case with the tort of passing off (discussed above).

Defence members engaging in social media for Private Use need to ensure that they do not use the registered trade marks of others (particularly famous or well known trade marks) in their communications where the use may be seen to be use 'as a trade mark'.

In circumstances where Defence invites the uploading of user-generated content from third parties as part of Professional Use, it will be very important to have clear rules of posting and then to censor the content to ensure that no well known trade marks are uploaded by third parties (see Engagement Principles below). While such use would often not be use 'as a trade mark' in the requisite commercial sense, and therefore would not

result in trade mark infringement, rules preventing the use of trade marks will go a long way to reducing the risk of complaint by trade mark owners and any associated adverse publicity.

To date, there have been no decided Australian cases in respect of the liability of social site or page owners arising from acts of trade mark infringement perpetrated by users. Clearly published Engagement Principles and a functional complaint and take down mechanism will go a long way to reducing any legal liability.

Copyright

Introduction

Copyright law in Australia is governed by the **Copyright Act 1968 (Commonwealth)**. By virtue of Section 7, the Copyright Act binds the Crown.

Copyright protects from unauthorised reproduction or adaptation of **original** creations such as books and other literary works, computer programs, scripts, lyrics, paintings, sculptures, drawings, photographs, musical scores, films, videos, broadcasts, sound recordings and the choreography of a performance. The copyright owner has the **exclusive right** to reproduce, copy, publish, perform, broadcast, adapt, sell, licence and import copyright protected creations. The copyright owner also has the exclusive right to communicate the work to the public (broadcast or place on the internet) and to reproduce the work in a material form.

The general rule is that the ‘creator’ of a literary, artistic, dramatic or musical work and the ‘maker’ of a film, sound recording, broadcast or published edition are the copyright owners. Exceptions to this general rule include situations where the creator is an employee of an organisation.

For example, copyright can exist in logos and marketing designs, compilations of data, advertising material, computer programs, digital images, digital video content and video games. Film may have up to seven different copyrights and music up to three different copyrights.

Copyright laws in Australia only protect the form of certain works, not the ideas, concepts, formats or themes behind them.

Copyright in original work or material may be infringed where an organisation or individual, without the copyright owner’s permission:

- reproduces the work in a material form;
- publishes the work;
- communicates the work to the public;
- performs the work in public (literary, dramatic and musical works);
- adapts the work;
- makes a copy of a sound recording, film or broadcast;
- communicates a sound recording, film or broadcast to the public; or
- causes a recording or film to be heard or seen in public.

Professional Use and Private Use – Use of Content in which Copyright Subsists

Defence will generally need to comply with copyright laws during Professional Use when uploading content to its own socially enabled websites, blogs and social media site pages. The same will apply to Defence members engaging in social media for Private Use. There is a common misconception that just because content can be freely viewed online, it can then be freely used. As indicated above under the heading User-Generated Content, this occurs regularly in ‘mashups’ posted in social media by individuals and sometimes commercial and non-commercial organisations.

Unless one of the exceptions outlined below applies in respect of a given piece of content, in order to avoid potential liability for copyright infringement, it is best practice to assume that copyright will subsist in most items of original content that were not created by Defence or its members and obtain permission for its use from the creator. Permission should be in writing from the copyright owner or a person who has the right to deal in the copyright, and one must satisfy themselves that the person they are dealing with actually has the right to deal with the material in this way. The permission obtained needs to cover the particular use as well as allowing publication on the required social media channels.

Whilst an item of content may enjoy copyright protection, infringement of copyright will only occur where a **substantial or important part** of an original work is copied. When assessing whether a ‘substantial’ part of a work has been copied, the rule of thumb is to consider the quality of the element that has been reproduced rather than the quantity of the original work that has been copied. A common example given to illustrate this point is reproducing the smile of Mona Lisa - while the smile itself is not a sizeable portion of the painting, its significance and intrinsic value to the painting renders it to be a substantial part of the original work.

Further, if there has been a commercial purpose for the use of the copied part, if the copied part has been taken to save labour or if the owner’s and copier’s works compete, this may also have a bearing on whether the part taken is ‘substantial’.

The courts have consistently held that names, titles, slogans or phrases are not protected by copyright, as commonplace words or sentences will not be ‘original’ for the purposes of copyright law. Longer quotes can be reproduced provided the quote is not a substantial part (defined as an essential, distinctive or important part) of the original literary work, or if the literary work from which the quote came is no longer protected by copyright). However, the **Competition and Consumer Act 2010**, trade mark laws and the laws of passing off discussed above often restrict the way an organisation or individual can use a quote, name, title or slogan, particularly if the organisation complaining has established a reputation in what has been reproduced. It is worth observing that simple descriptive or editorial references to well known names, titles or slogans in social media (e.g. in a blog post or comment on Facebook) are unlikely to attract the attention of such laws.

If content is no longer protected by copyright, then it may also be freely used by Defence or its members in social media. Generally, the rules prior to 1 January 2005 were that copyright lasted until 50 years from the end of the year in which the creator died, or for some material, until 50 years from the end of the year in which the material was first published. Since 1 January 2005, works created or published on or after 1 January 1955 enjoy copyright protection to 70 years from the end of the year in which the creator died or 70 years from the end of the year in which the material was first published.

As far as content to be used in social media is concerned, the general rule is that if the creator of the content died before 1955, copyright in the content is likely to have expired under Australian law. While the expiry of copyright may be useful for some who wish to upload vintage content in social media, the vast majority of those engaged in social media seek to upload contemporary and relevant content. Subject to this content being an original work, copyright is likely to subsist in the content and care must be taken with its use.

It is recommended that Defence and its members ensure that they have permission (i.e. a licence) to use content that may be subject to copyright before creating user-generated content and deploying such content in social media. If unsure as to who might own an item of content or if you do not know who is in the image or video, it is best practice not to use the material in social media.

Social Media Sites: Linking & Framing

The essential architecture of the Web itself enables users to ‘surf’ the Web by clicking hyperlinks within website pages or from website to website through the use of hyperlinks.

It may be of importance to Defence in its Professional Use of social media to be associated with other government organisations, NGO’s, businesses and individuals with whom Defence has established relationships. Through hyperlinks, legitimate associations between Defence and such organisations can be promoted via the Web. Furthermore, engagement in social media often involves the provision of links to newspaper stories, other blogs, content on YouTube and so on.

Where a website hyperlinks to the homepage of a target website, this is often referred to as **surface linking**. Framing occurs where a website contains a hyperlink to another site and when an individual clicks the link, the new site opens up in its own window but within the existing screen (i.e. the original website remains in the background and is clearly visible). This is the ‘frame’. Numerous frames can be viewed in separate parts of the screen at the same time while still functioning independently of each other.

Hyperlinks and framing also provide an opportunity for some organisations to derive a benefit or advantage by associating themselves with another organisation or their Web content without permission. For some time now, a rogue practice known as ‘deep linking’ has been utilised. As opposed to surface linking, deep linking occurs where an offending website links to an internal page within a target website that is not the target website’s homepage. Often the target website’s internal page is framed upon the offending website’s page making it look like they are part of the same website. The offending website often

obtains a benefit from the association or the content that resides within the target website. Further, the practice of deep linking usually bypasses the disclosures, terms and conditions and disclaimers that appear on a homepage, and therefore individuals also have the potential to be misled.

The Australian authorities support the view that linking or deep linking on its own is unlikely to raise issues under copyright law. This is because an organisation that provides hyperlinks on their website to content stored on remote websites does not make that content available, rather it is the remote website that makes the content available and thus there is no reproduction (one of the exclusive rights). However, if the links are to target sites that host infringing content there may be liability for authorising infringements (see below). Furthermore, unless embedding is expressly allowed by the social media site owners (e.g. the YouTube Embeddable Player) framing may also raise copyright concerns, as the viewer of the framed content may not be aware that the content has been drawn from a different source. This may result in the communication of a copyright work (another of the exclusive rights) albeit not a reproduction of that work.

It is therefore best practice to link and frame with the permission of the target site or in accordance with the target sites published rules and policies. As there is always a risk in social media that people will post links to infringing material, procedures need to be in place to manage risk if Defence is inviting or allowing such posts (see Engagement Principles below).

The practice of unauthorised linking or framing may result in an infringement of the other relevant laws, including:

Moral rights. The framing of or linking to content on a target website may lead to confusion as to ownership, which may infringe the copyright owner's right of attribution or the right not to have authorship falsely attributed. If framing results in the target website's content being displayed in close proximity to offensive content upon the offending website, the copyright owner's right not to have work subject to derogatory treatment may also be infringed.

Trade mark infringement. Usually the mere use of a trade mark as a bare link will not be use 'as a trade mark' in a way that gives rise to infringement under the **Trade Marks Act**. However, if framing occurs and the target website's trade marks are displayed within the offending website's screen, this may result in use as a trade mark. Further, if the target website's frame within the offending website suggests some form of association between the trade mark and the products promoted on the offending website, trade mark infringement may occur.

Consumer protection laws. Under the **Competition and Consumer Act 2010** all that needs to be shown is that the nature of the linking and framing (including appearance of logos, titles and URLs) may result in a person being misled (Section 18). This could occur if the person is unaware that he or she has accessed the target website. In addition, the proximity and representation of the content, logos and trading names of the offending and innocent websites may suggest an association that does not exist (infringing Section 29).

Passing off. The elements of a passing off action may also be established by the owner of the target website in circumstances where the proximity and representation of the content, logos and trading names of the offending and innocent websites transgresses upon the innocent party's goodwill.

When establishing links and frames on and from a website:

- always obtain permission from the target website;
- ensure that the organisation's webpage does not imply an endorsement or connection with a target website, a personality, an individual or another business or the products of others unless there is permission;
- do not use names, trade marks, brands, products and slogans of other organisations; and
- do not use deep linking where the hyperlink avoids important disclosures or conditions of the target website's homepage (or similar).

Authorisation Liability for User-generated Content

As discussed above, engagement in social media necessarily results in the creation of user-generated content. One of the risks Defence and Defence members face in inviting or allowing user-generated content during both Professional Use and Private Use is that of copyright infringement as an 'authoriser' of primary copyright infringement.

The exclusive rights of a copyright owner include the right to authorise another person to do any of the acts falling within the scope of the copyright owner's exclusive rights (discussed above). So if a person or organisation authorises another person to do the acts without the licence or consent of the copyright owner, 'authorisation liability' may arise.

Whilst well known commercial content mashed up or contained within a content submission will readily be detected and intercepted, it is possible that ordinary or unknown content submitted by an individual will not be owned by that individual or used with the owner's permission, resulting in copyright infringement. As this type of content is almost impossible to detect during the censorship process, it is likely that it will be published by Defence on the site and this is the likely point that authorisation liability may occur. In such circumstances Defence may also be directly liable for copyright infringement by reproducing the material on its servers or for communicating the work.

Under Section 36(1A) of the **Copyright Act 1968**, the following matters will be taken into account in determining whether or not a person has authorised the doing of any act comprised in the copyright in a work:

- the extent of the person's power to stop the infringement;
- the nature of the relationship;
- whether the person took any reasonable steps to prevent or avoid the doing of any act comprised in the copyright in a work.

The likelihood of copyright infringement taking place and the degree of indifference displayed by the organisation alleged to have authorised the infringement are relevant in determining liability. The Engagement Principles recommended below will assist greatly in this regard.

It is outside the scope of this overview to enter into a detailed examination of the so called ‘safe harbour’ provisions under the **Copyright Act 1968** (Part V, Division 2AA) that received detailed attention in the much publicised iiNet cases (**Roadshow Films Pty Ltd v. iiNet Ltd (No.3)** [2010] FCA 24 and on appeal **Roadshow Films Pty Ltd v. iiNet Ltd** [2011] FCAFC 23). In short, these provisions limit the remedies available against carriage service providers for copyright infringement that occurs in connection with carrying out certain specified online activities. Generally such carriage service providers are often internet service providers (such as Telstra, Optus, Vodafone, iiNet and AAPT). The safe harbour provisions do not extend to organisations that own or run websites.

In circumstances where Defence invites the uploading of user-generated content from third parties as part of Professional Use it will be very important to have clear rules of posting and then to censor the content and include a functional copyright complaint mechanism to deal with allegations of copyright infringement on the site (see Engagement Principles below).

It is worth mentioning that there are a number of ‘fair dealing’ provisions in the **Copyright Act** that provide that certain acts will not constitute infringement of copyright. Such provisions can apply to the user-generated content environment and in certain circumstances may apply to Professional Use and Private Use of social media by Defence and its members.

The relevant ‘fair dealing’ provisions are as follows:

Reporting the News: the use of the material must be ‘fair’ and the primary purpose must be to report or comment on news and not for example to entertain. It is also necessary to ensure that an acknowledgement of the person who created the content and any title is given unless the content is anonymous.

Criticism or Review: the use must be ‘fair’ and the criticism or review must involve making a judgment upon the content concerned or the underlying ideas. The purpose of the criticism or review must be genuine. A commercial motive underlying the criticism or review may still result in copyright infringement.

Parody or Satire: there is no definition of parody or satire in the Copyright Act so we must wait until a court has decided the meaning, although the Macquarie Dictionary defines ‘satire’ as the use of irony, sarcasm, ridicule denouncing vice or folly etc. and ‘parody’ as the humorous or satirical imitation of a serious piece of literature or writing. The use must be ‘fair’ and this may depend upon how much content is used, the context and if the copyright owner may suffer some form of commercial disadvantage. Just because an individual uploads user-generated content that has used copyright material in a humorous way does not necessarily mean that the use is covered by this exception. The ability to rely upon this exception must be balanced against the moral rights provisions (see Moral Rights below).

For the fair dealing provisions to apply the use must be 'fair' in the requisite sense. The Courts will look at whether the use was genuinely for one of the above fair dealing exceptions and the circumstances of the use including whether the use of the content was for commercial purposes, the circumstances of acquisition of the content and any detriment to the copyright owner.

Moral rights

In Australia there is a parallel set of rights to copyright which authors, creators and performers enjoy, known as moral rights. They were introduced into Australian copyright law by the **Copyright Amendment (Moral Rights) Act 2000 (Commonwealth)**.

Moral rights exist independently from the copyright that may exist in original material and may continue to be exercised by an author or performer even though the copyright ownership has transferred to another person. The key moral rights recognised are:

The right of attribution of authorship or performership – i.e. the right to be identified as the author of a work or performer of a live or recorded performance.

The right not to have authorship or performance falsely attributed – i.e. the right to prevent a person falsely suggesting or stating that they are the author of a work or performer.

The right of integrity of authorship or performership – i.e. the right not to have the work or performance subject to any derogatory treatment.

Moral rights only apply to individuals and these rights can be waived by the person who holds the rights. Further, the holder of the rights can consent to a breach of the holder's moral rights on a case by case basis. Recent changes to the Copyright Act have granted moral rights to performers such as dancers, actors and musicians as well as the original group of writers, composers and directors.

For the right of integrity to be infringed, the distortion or alteration to the material must be prejudicial to the author's honour or reputation. Further, there is no breach of the right of attribution or of the right of integrity if an organisation or individual is able to establish that in the circumstances it was reasonable not to identify the author or that it was reasonable to subject the work to derogatory treatment, as the case may be.

Defence and its members who engage in social media for both Professional Use and Private Use have to understand that they may have to attribute third party material and be particularly careful if their intention is to retouch, edit, alter or distort third party content as part of mashups with their own user-generated content. Again, it is best to seek permission from the rights holder or alternatively, ensure that the alteration to the material or any derogatory treatment is reasonable in the circumstances.

In **Meskenas v ACP Publishing Pty Ltd** [2006] FMCA 1136, one of the first cases of its kind in Australia, ACP Publishing was found to have infringed an artist's moral rights to be

attributed as the author of a painting. ACP published a photo in Woman's Day magazine of Princess Mary during a visit to the Victor Chang Cardiac Research Institute in Sydney. The photo showed the princess standing in front of a portrait of the late Dr Chang painted by the artist but the caption to the photo incorrectly attributed the painting to another artist. ACP failed to publish an apology in time and had to pay the artist damages.

Defamation

Defence and Defence personnel need to be conscious of the possibility that their social media communications in both Professional Use and Private Use may offend a particular individual or group of individuals to such an extent that they allege that they have been defamed as their character and reputation has been diminished by the portrayal of them.

Defence will need to be particularly vigilant to ensure that user-generated content uploaded to Defence sites or pages by individuals during Professional Use of social media does not defame an individual. This would apply in particular where a communication portrays a well-known public figure, corporate figure or celebrity.

Defamation occurs where one person communicates, by words, photos, video, illustrations or other means content which has the effect or tendency of damaging the reputation of another. Every person who authorises the publication of defamatory material or contributes to the publication of defamatory material, regardless of the precise degree of involvement, may be liable. Liability for participating in the publication can extend to organisations and individuals who own and operate traditional websites, chatrooms, blogs, wikis, podcasts or pages on the social media sites (for example, Twitter and Facebook).

Australia adopted uniform **Defamation Acts** in 2006 as part of ongoing law reform. Broadly speaking, under the uniform defamation laws you can say whatever you like about someone, no matter how private, sensitive or personally damaging it may be, as long as it is true and the truth can be proven if the matter goes to court.

Liability for a defamatory publication may also extend to situations where there has been a failure to prevent or terminate a publication by a third party, for example in the case of a defamatory statement posted for example to an internet bulletin board, blog site or social media site. If the owner of the website or social media page that allows user-generated content including commentary and postings, exercises or should be able to exercise editorial control over the postings and then allows defamatory material to remain on the website, the site or page owner could also be liable for defamation.

Notwithstanding a uniform national approach, defamation law remains very complex and a full discussion of defamation is well beyond the scope of this overview. However, Defence and its members need to be aware that the possibility of defamatory statements being published over the internet is very high due to the ease with which statements can be made and communicated.

For example, the humorous or satirical portrayal of well known public figures, corporate figures and celebrities remains popular in social media. Whilst there is a defence of 'triviality' in the Defamation Acts – if you are able to prove that the publication really caused no harm – merely because something is published in jest does not prevent cartoons, caricatures, jokes or satire from being subject to the laws of defamation.

It is the interpretation of the ordinary reader/listener/viewer and not the intention of the author that matters. If the ordinary person would interpret the communication as mere jest there will be no defamation. However, if the communication holds its subject up for ridicule (which is often the case) or where the attempted humour promotes a sinister underlying assumption of truth which might be defamatory, the author cannot claim that the communication was no more than comic nonsense.

It is worth mentioning that since the adoption of uniform laws in 2006, it is generally only living individuals that can sue for defamation and corporations are now unable to sue for defamation except if they employ fewer than 10 persons.

There are currently no decided Australian cases on the liability of internet intermediaries (internet service providers e.g. Telstra or iiNet and internet content hosts e.g. Facebook or Flickr) or site owners generally for defamation that is perpetrated by another person using their services or facilities. It is however well established in Australian law that the law of defamation applies in cyberspace and to internet publications and that the place of the defamatory publication will be the place where the online material is read or heard in a comprehensible form (High Court in **Dow Jones & Company Inc v Gutnick** (2002) 210 CLR 575).

The situation of anonymous posters on third party owned internet sites was recently considered in **Moir & Datamotion v Gladman**. In January 2010, IT company Datamotion Asia Pacific Limited (Datamotion), and its managing director, Mr Ron Moir commenced proceedings in the Western Australian Supreme Court in relation to defamatory material published about them on the internet forum HotCopper Australia (HotCopper). HotCopper is a forum in which online discussions take place in relation to companies whose securities are traded on the Australian Securities Exchange.

The defamatory material consisted of a series of defamatory posts by an anonymous user in various HotCopper discussion threads about Datamotion and Mr Moir.

Due to its privacy and confidentiality policy, HotCopper would not voluntarily disclose details it held in relation to the anonymous poster. Datamotion and Mr Moir obtained court orders against HotCopper's owner which required disclosure of information about the anonymous poster under a pre-action discovery process. The information provided by HotCopper started a train of inquiry which led to the uncovering of the anonymous poster's identity, proceedings for defamation being issued against him and the case quickly being resolved.

Analogous to defamation is the action of injurious falsehood, with an example of the risks website owners face highlighted under the Injurious Falsehood discussion below.

It is important to remember that social media has a very long memory and user-generated content is likely to remain embedded in cyberspace for a very long time. Further, the ubiquitous nature of social media increases the likelihood of a defamatory communication spreading quickly across the globe and being ‘published’ to many people, particularly if the content goes ‘viral’. This can only increase the liability of an organisation or individual in the event that a communication contains defamatory content.

As with copyright, in circumstances where Defence invites the uploading of user-generated content from third parties as part of Professional Use, it will be very important to have clear rules of posting and then to censor and remove offending content and include a functional complaint mechanism to deal with allegations of defamation (perceived or real) on the site (see Engagement Principles below).

The case of **Moir & Datamotion v Gladman** demonstrates that Defence members when engaging in Private Use in social media may not be able to hide behind handles and anonymous postings should they decide to defame or ridicule an individual or organisation. Likewise Defence may be required to disclose the identities of contributors to its websites or social pages if posted user-generated content is defamatory and an individual brings Court proceedings, notwithstanding privacy obligations upon Defence (see below).

The implementation of appropriate Social Media Policies covering Professional Use and Private Use and Engagement Principles (discussed below) will assist in educating Defence members and third parties alike on appropriate social media conduct.

Discrimination, hate speech & causing offence

Defence and Defence personnel also need to be conscious of the possibility that their social media communications in both Professional Use and Private Use may be caught by the various Commonwealth, State and Territory discrimination and racial vilification laws and possibly even the Commonwealth Criminal Code.

In addition to censoring for defamatory statements, Defence will need to be particularly vigilant to ensure that user-generated content uploaded to Defence sites or pages by individuals during Professional Use does not contain content that is discriminatory or harassing or contain statements based on racial or religious grounds. Such content must be immediately removed from the site or page.

For example the **Racial Discrimination Act 1975 (Commonwealth)** provides in Section 18C that it is unlawful for a person to do an act, otherwise than in private, if:

the act is reasonably likely, in all the circumstances, to offend, insult, humiliate or intimidate another person or a group of people; and

the act is done because of the race, colour or national or ethnic origin of the other person or of some or all of the people in the group.

In **Jones v Toben** [2002] FCA 1150 the Federal Court found that the respondent had breached Section 18C by publishing material online which was reasonably likely, in all of the circumstances, to offend, insult, humiliate and intimidate Jewish Australians

or a group of Jewish Australians. The Court was further satisfied that the respondent published the offending material because of the ethnic origin of Jewish Australians. The Court made an order declaring that the respondent engaged in conduct rendered unlawful by the Racial Discrimination Act and made orders requiring the respondent to remove the offending material, and any other material the content of which is substantially similar to the offending material, from all internet sites controlled by the respondent and not to publish or republish such material.

The Commonwealth Criminal Code, updated through the **Crimes Legislation Amendment (Telecommunications Offences & Other Measures) Act (No. 2) 2004**, features offences of using a carriage service 'to menace, harass or cause offence'.

The offence is found in Section 474.17 of the Code:

474.17 Using a carriage service to menace, harass or cause offence

(1) A person is guilty of an offence if:

(a) the person uses a carriage service; and

(b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.

Penalty: Imprisonment for 3 years.

'Carriage service' has the same meaning as in the **Telecommunications Act 1997 (Commonwealth)** Section 7, being a service for carrying communications by means of guided and/or unguided electromagnetic energy. This definition is broad enough to capture telephone calls, email, SMS and other online communications. Individuals using social media and other related communications channels to menace, harass or cause offence may be liable to prosecution under this offence provision.

The implementation of appropriate Social Media Policies (discussed below) covering Professional Use and Private Use will assist in educating Defence members on appropriate statements to make in social media.

Finally, it is worth mentioning that extant Defence policies on equity and diversity may also need to be examined and revised in order to ensure that Defence members understand their responsibilities to each other during Personal Use of social media. Equity and diversity in Defence as an organisation is an important but broad area that encompasses legal as well as cultural issues. The impact of social media upon equity and diversity policy in Defence is presently beyond the scope of this overview and will need to be examined in greater detail once Defence has indicated how it intends to embrace and engage in social media as an organisation following consideration of the preliminary George Patterson Y&R Social Media Review.

Injurious falsehood

Whilst defamation is primarily concerned with the protection of reputation of an individual, Defence and its members also need to be conscious of a related legal action known as the tort of 'injurious falsehood' that can be brought by commercial entities.

An injurious falsehood case may be brought against an organisation or individual where it is alleged that their communications contain false statements concerning the property, goods or services of another person or entity.

An aggrieved person or entity will succeed in such an action where:

- the communication contains a false statement concerning the person's products or business;
- the communication is published in the marketplace;
- the organisation or individual acted with some malice; and
- as a result of the false statement, the person has suffered some actual financial loss.

Kaplan v Go Daddy Group Inc [2005] NSWSC 636 involved the tort of injurious falsehood. The defendant created a website with the domain www.hunterholdensucks.com.au and a disparaging blog about Hunter Holden that encouraged other users to post derogatory comments about this business. Comments were posted to the blog, all of which contained defamatory comments about the business. The plaintiff applied to the Court for an injunction to prevent the defendant from maintaining the defamatory blog. The Court granted the injunction saying that there was a serious question to be tried as the defendant had committed and threatened to commit the tort of injurious falsehood by posting the derogatory comments about the plaintiff in his blog.

Again, the law of injurious falsehood is complex and a full discussion is well beyond the scope of this overview. However, Defence and its personnel need to be aware of the possibility of injurious falsehood being alleged in response to social media communications. Clearly published and enforced Engagement Principles will go a long way to reducing risk in this regard.

Privacy laws

Many individuals are concerned about the collection and use of their personal information, particularly in respect of the internet and mobile technologies.

For instance, social media has the ability to create sophisticated consumer profiles

from the information provided unknowingly by internet and mobile users. As technology enables large volumes of data to be collected, stored and accessed quickly and easily, organisations have been quick to capitalise upon the different ways in which personal information can be used.

In addition, individual privacy has been further eroded by the proliferation of digital cameras, mobile devices with camera and video capabilities, the rise of user-generated content websites, improved search engines and the indexing of internet content. Personal information can now be captured in digital form, uploaded and then retrieved with ease.

Many of these technologies have a real or potential impact upon privacy. New challenges to privacy are now presented by digital rights management, geo-location technologies and computing in the 'cloud'. Concerns continue to be raised due to high profile incidents involving the disclosure of personal information such as names, addresses, credit card details and social security numbers. The information disclosed by users of the social media sites, particularly Facebook and Twitter, has also raised privacy concerns. Individuals that engage with social media post a significant amount of information about themselves and others online that can be collected and reassembled to create accurate profiles of individuals and their lives, habits and preferences.

At this time there is no general right to privacy under Australian law. Personal information is protected under a mix of Commonwealth, State and Territory laws and the actions for breach of confidence and if applicable, contract law. Furthermore, some recent lower Australian court decisions have recognised a limited tort of invasion of privacy in Australia.

The privacy laws that predominantly impact upon the activities of the private sector are to be found in the **Privacy Act 1988 (Commonwealth)** which was amended in late 2001. On 21 December 2001 the private sector amendments to the Privacy Act became operative. The amendments provided for ten National Privacy Principles (NPPs), found in Schedule 3 of the Privacy Act, which apply to the private sector. At this time the Privacy Act does not apply to organisations that are small business operators (a business with an annual turnover of \$3 million or less) or registered political parties.

The Privacy Act also applies to Australian and Australian Capital Territory government agencies through the Information Privacy Principles (IPPs) set out in Section 14 of the Privacy Act. There are 11 IPPs that set out how government agencies may collect, use, store and disclose 'personal information' which is defined in Section 6.

The 11 IPPs are as follows:

- Principle 1 - Manner and purpose of collection
- Principle 2 - Solicitation of personal information from individual concerned
- Principle 3 - Solicitation of personal information generally
- Principle 4 - Storage and security of personal information
- Principle 5 - Information relating to records kept by record-keeper
- Principle 6 - Access to records containing personal information
- Principle 7 - Alteration of records containing personal information

Principle 8 - Record-keeper to check accuracy etc. of personal information before use

Principle 9 - Personal information to be used only for relevant purposes

Principle 10 - Limits on use of personal information

Principle 11 - Limits on disclosure of personal information

Whilst the IPPs apply to Defence, including any engagement in social media for Professional Use where personal information may be collected, it is unlikely that the NPPs would apply to Defence members collecting personal information during Private Use of social media.

Government agencies are expected to set high standards for information handling. This is because, unlike other sectors such as the private sector, individuals may not have alternatives or substitutes to the services performed or provided by government and may have no choice other than to provide their personal information. Thus in the social media context it will be particularly important for Defence to publish privacy notices that comply with the IPPs at the point of collection of personal information.

Privacy Law Reform

At the time of writing, the Privacy Act is limited in its application to the protection of 'personal information', which is defined in Section 6 as:

'information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.'

The problem with the definition as it currently stands is that it is unlikely to apply to technology which makes it possible to process data relating to individuals that is not linked to their immediate identity. While the definition covers a person's name, address date of birth, telephone number, family members, photos or videos, most commentators are of the view that the definition does not cover an individual's IP address, mobile telephone number and email address.

On 31 January 2006, the Australian Law Reform Commission (ALRC) commenced an enquiry into the extent to which the Privacy Act and related laws continue to provide an effective framework for the protection of privacy in Australia. A final report was delivered to the Australian Attorney-General in late 2008. The Government released the first stage of its response to the ALRC Report 108 on 14 October 2009.

On 24 June 2010, the Government released exposure draft legislation containing an important element of the first stage response – the proposed Australian Privacy Principles (APPs), which unify the current Information Privacy Principles and the National Privacy

Principles. These proposed principles were tabled in the Senate for referral to the Senate Finance and Public Administration Committee. The Committee held public hearings on the Principles on 25 November 2010, and the Committee's report was tabled on 15 June 2011, with a final reporting date of 30 September 2011. On 31 January 2011, the Government referred the second component in the first stage of the Government's privacy reforms, the credit reporting provisions, to the Senate for tabling, and for referral to the Finance and Public Administration Committee to consider. Stage 2 of the Government's response will consider the remaining recommendations in the ALRC report once the first stage reforms have been progressed.

The 13 new APPs apply to 'entities', that is, Federal Government agencies and private sector organisations. The APPs expand the obligations upon government and business and increase privacy protections from that currently existing in the IPPs and NPPs.

One element of Privacy Act reform is the new definition of 'personal information'. The new definition contained in Section 15 of the APP's provides as follows:

'Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- (a) whether the information or opinion is true or not; and
- (b) whether the information or opinion is recorded in a material form or not.'

It is likely that this definition will result in a significant expansion of coverage of the Privacy Act as the test for what is 'personal information' moves away from precise identity to simply being able to identify a person indirectly. This is likely to occur when an individual visits a website on more than one occasion and through the use of IP addresses, cookies, web bugs, Hypertext Transfer Protocol (HTTP) and spyware the individual is reasonably identifiable through his or her browsing behaviour.

If personal information is being collected during social media engagement, then the APPs will need to be complied with. Of particular importance to Defence during Professional Use include the following proposed APPs:

APP 1 – Open and transparent management of personal information. This principle expressly mandates that an entity must have a clearly expressed and up to date privacy policy covering specified matters including how information is collected, how to complain and the purposes for which the entity collects, holds, uses and discloses personal information.

APP 2 – Anonymity and pseudonymity. This principle provides that individuals should be permitted to interact with entities while not identifying themselves or by using a pseudonym, where it is lawful and practical to do so.

APP 3 – Collection of solicited personal information. Entities must not collect

personal information unless it is reasonably necessary for, or directly related to, the entity's functions or activities. Defence will need to carefully consider this on a case by case basis.

APP 4 – Receiving unsolicited personal information. If an entity receives unsolicited personal information, the information is still afforded privacy protection and the entity must then determine if it had the right to collect the information under APP 3 and if so the balance of the APPs would apply. It is important to consider APP 4 in the context of social media engagement where unsolicited personal information may be disclosed by individuals to Defence.

Thus in the course of engaging in social media for Professional Use, Defence will need to ensure that an up to date privacy policy is available for viewing and download (free of charge) at the point of collection of personal information. Further, Defence will need to carefully consider in light of APP 2 whether it will mandate the need for individuals to disclose their identities if they wish to post comments, blogs or upload user-generated content during social media engagement. Defence may not consider it practical to allow pseudonyms due to the risks of copyright infringement, defamation or a breach of one of the other laws identified in this overview. Indeed, the disclosure of identity is recommended in the Engagement Principles outlined below.

Images of Third Parties in User-generated Content – Privacy Considerations

Often user-generated content uploaded during the course of social media engagement will contain images of individuals who may not necessarily be the individual uploading the content. Such individuals will often be the uploader's friends or family members but on other occasions the individuals may also be unknown third parties that were caught in the background or were deliberately captured by the uploader during an event of interest.

The Engagement Principles suggested below make it a positive obligation upon the uploader to agree that no content will be uploaded unless all individuals depicted in the content have granted their consent or would otherwise expect their image to be used by the uploader in social media. However, it will not usually be practicable to confirm such consent. If Defence invites image-based user-generated content during Professional Use the privacy implications need to be considered if the third parties have not provided the necessary consent to the upload.

In this context it is important to ask whether there are any rights in Australia that people have to protect their 'personality' or their 'image' from use in social media. Under Australian

law there is no specific law aimed at preventing the unauthorised use of a person's image (unlike the United States which has **right of publicity** laws which provide that an individual has the right to control and profit from the use of his/her name, likeness and persona).

Copyright law is of little assistance in preventing unauthorised use of an image because the person who owns the copyright in the social content will generally be the person that created and uploaded the content rather than the person who appears in the content.

The areas of law in Australia which may be used by an individual to try and prevent the unauthorised use of his or her image are as follows:

Defamation. The publication of a person's image without their consent is not in itself proof of defamation. The unauthorised use of the image would need to either lower the public's estimation of the person, expose the person to hatred, contempt or ridicule, or cause the person to be shunned or avoided.

The Competition and Consumer Act 2010. Sections 18 and 29 prohibit commercial conduct which misleads or deceives consumers. To prevent the unauthorised use of an image under this law it is necessary to show that the use of the image would mislead or deceive consumers. The mere use of a person's image is unlikely to be found to mislead or deceive under this area of law unless that person is a celebrity or well-known endorser of products. If a person is a celebrity or otherwise well-known, then the unauthorised use of their image in connection with trade or commerce may constitute misleading or deceptive conduct. This is because the public would be led to believe that the celebrity is endorsing the product or is connected somehow with the site upon which the image was uploaded. If there is nothing in the unauthorised use of the image which misleads or deceives a court would not find in favour of the person whose image is used.

Passing off. The law of passing off is designed to protect the reputation of a business from misrepresentation and the possibility of an opportunity to exploit a person's image for gain. To succeed in an action for passing off the complainant must have a reputation and there must be a misrepresentation which causes damage or the likelihood of damage to the individual. Because a reputation is required to successfully establish passing off, this law is of limited use for the 'average person in the street'.

Privacy Act. If the image of the third party and any associated text or content results in the individual being 'reasonably identifiable' then this may constitute 'personal information' for the purposes of the new APPs. If so, the image may be unsolicited personal information for the purposes of APP 4 and would need to be handled in accordance with the APPs.

Invasion of privacy. Whilst there is no right to privacy in Australia, some recent developments in the Australian courts leave open the possibility of a future or limited tort of invasion of privacy in Australia. A tort is a private, civil wrong or injury for which the court may provide a remedy for any damage caused. The tort would only apply where the information disclosed was of a private nature and often images of persons are taken with their knowledge for the purpose of being shown.

As with the other laws influencing and restricting Defence engagement in social media for Professional Use, where Defence invites the uploading of user-generated content from third parties as part of Professional Use, it will be very important to have clear rules of posting and then to censor and remove offending content and include a functional complaint mechanism to deal with privacy complaints on the site (see Engagement Principles below).

SPAM laws

The sending of 'commercial electronic messages' in Australia is governed by the **SPAM Act 2003 (Commonwealth)**.

A basic definition of 'commercial electronic message' is provided by Section 6 which essentially provides that some commercial nexus is required, through offering to supply goods or services or advertising or promoting goods, services, land, prospective suppliers or business opportunities. Under the SPAM Act, commercial electronic messages include messages sent by way of email, IM (Instant Messaging) and Mobile Wireless Technology (MWT) including SMS (Short Message Service), MMS (Multimedia Message Service), Wireless Access Protocol (WAP) and 3rd Generation technology (3G).

The SPAM Act prohibits the sending of commercial electronic messages to an individual unless that individual has consented to receiving such communications. That consent can take the form of 'express consent' or 'inferred consent'.

Whilst the Spam Act binds the Crown in each of its capacities and applies to government departments, the occasions upon which Defence would actually need to send commercial electronic messages may be somewhat limited. To prevent any unintended restriction on communication between Government and the community, the Spam Act contains a limited exemption for some commercial electronic messages sent by government bodies. These messages are called 'designated commercial electronic messages'. Defence will need to consider the application of the Spam Act on a case by case basis.

In the social media context it is unlikely that Private Use of social media would often attract the requirements of the Spam Act. Defence may need to consider the application of the Spam Act if, as part of its Professional Use, it collects through social media engagement email addresses and mobile telephone numbers in order to generate a database of individuals who are interested in Defence and its activities and wish to be kept up to date with Defence related matters including news, articles or recruitment drives.

Whilst such communications may not often have a sufficient commercial nexus to be caught by the definition of 'commercial electronic message', Defence should be seen to meet and exceed the high standards expected of business. Thus it is always best practice to comply with the Spam Act requirements for individuals to have 'opted in' to receiving such communications from Defence to confirm consent and for each electronic message to contain accurate sender information (including how Defence can be contacted) and contain a functional unsubscribe facility.

Recordkeeping Obligations

Defence should also be aware that its social media communications arising from Professional Use are likely to generate Commonwealth records that will attract auditing, recordkeeping and disclosure obligations under the numerous Commonwealth acts and regulations that can apply to Defence.

Key auditing, recordkeeping and disclosure legislation applicable to Defence includes the following:

- Archives Act 1983;
- Freedom of Information Act;
- Privacy Act 1988;
- Evidence Act 1995;
- Public Service Act 1999;
- Financial Management and Accountability Act 1997;
- Auditor-General Act 1997; and
- Commonwealth Authorities and Companies Act 1997.

Given the dynamic nature of social media communications and the collaborative approach to the creation of user generated content, Defence will need to take particular care to ensure that such content is properly identified as a Commonwealth record as and when it is created. An accurate and authentic copy of such content will need to be captured and saved as a record so as to ensure that obligations under the relevant auditing, recordkeeping and disclosure legislation can be met. This is likely to require the development of a specific Defence social media records policy that provides guidance for each particular social media channel to be used by Defence during Professional Use.

The specific application of such legislation and the development of policy to regulate Professional Use of Social Media by Defence should be examined and will need to be considered further once Defence has indicated how it intends to embrace and engage in social media as an organisation following consideration of the preliminary George Patterson Y&R Social Media Review.

The rules of proprietary space

The numerous mainstream and niche forums, blogs, file sharing and social networking sites are all owned and operated by entities and companies who govern the terms and conditions of use and set rules that the user community must follow. As such this property may be referred to as 'proprietary space'.

Defence will be well aware that most social sites offer their own unique social media communications options and solutions. Organisations no longer have to encourage

individuals to independently visit their Facebook page, YouTube channel or Twitter site. Today we see the social media sites becoming a key part of an organisation's site and this in turn broadening their engagement and exposure in social media. For example, the Defence homepage at www.defence.gov.au already has links to its Flickr, Twitter and YouTube pages.

As a condition of using proprietary space for communications, Defence must not only comply with the applicable laws discussed in this overview, but must also agree to the legal terms, conditions and policies set by the propriety space owners. As such terms and conditions constitute a contract between the site and user, they act in a very real way to influence and restrict communications activities upon proprietary space.

The particular rules of each proprietary space site are important for Defence to understand as they often reinforce the applicable laws and the consequences of a breach of the rules of proprietary space can sometimes be quite severe, including suspension and account termination. The rules must be examined carefully as they are prepared by the owners of proprietary space and are always drafted in their favour. These rules govern all aspects of use and are often changing.

As Defence continues to engage with individuals and other organisations on the social media sites for Professional Use it must constantly monitor the current rules and terms of use to ensure that the intended use is permitted and to determine what limitations on the use of the social media features may apply.

Social media engagement principles

The 'Engagement Principles' refer to terms and rules upon which Defence agrees to allow individuals and other organisations to engage with Defence in social media. In a similar way to the operation of the rules of propriety space employed by the social media site owners, the Engagement Principles should reflect the applicable laws and regulations that apply to Defence and operate in a practical way as part of an overall strategy to reduce the legal and reputational risks associated with the social media engagement identified.

Furthermore, the Engagement Principles form part of a suggested holistic approach to risk management in social media. Whilst the Engagement Principles govern how the outside community may engage with Defence, the Social Media Policies discussed below govern how Defence and its members engage with the outside community and with each other. This combined approach will enhance legal compliance and reputational awareness, engender a culture of appropriate 'netiquette' and reduce the risks for all stakeholders.

The suggested Engagement Principles for Defence to consider before committing to a social media communication or engagement campaign for Professional Use are as follows:

To minimise legal risks, Defence should be prepared to consistently monitor its sites and pages for derogatory or otherwise harmful content and if such content is posted remove it immediately, block the offender (if possible) and take any other reasonable action.

Each social media site or channel is unique enabling Defence to engage with individuals in different ways. Furthermore, each social media communication will also be unique. Therefore Defence will need to conduct an appreciation to consider applicable laws, assess risks and thereby determine most appropriate courses of action. Defence must assess the suitability of the social media channel for its intended communication and ask the question – ‘is social media suitable?’

As part of this process Defence will need to assess the type of individual that will be engaged and the reaction and participation of the individual. As part of this process it is vital that Defence has a public relations engagement plan ready to go once a social media campaign goes live that provides guidance how to respond to:

- praise;
- complaints;
- questions; and
- general conversation.

A public relations plan that addresses response times, issue resolution protocols and provides a process for handling enquiries will ensure that any emerging legal and publicity issues are diffused if possible and not compounded.

Where possible do not allow user-generated content to be posted anonymously by requiring individuals to identify themselves through a registration process. This will act as a strong deterrent against breaches of the Engagement principles. Such identifying information should include real names, address and telephone number as well as email address although this information should not be available to third parties.

Ensure that banner ads, Facebook ads, YouTube links / channels and all other seeds in social media that grab the attention of individuals to drive them back to Defence’s ‘home base’ website, Facebook page or blog do not contain tricks or other deceptive elements.

Beware of tricky communications that may go beyond mere wonderment or confusion and become misleading to others.

Ensure that all user-generated content is censored before being allowed to ‘go live’ or at least monitored for obvious legal infringements or breaches of the

Engagement Principles Defence has set. Obvious legal infringements should be immediately removed.

Remove obvious infringements of commercial content in 'mashups' (written, aural or visual).

Remove content that tends towards being defamatory to an individual, injurious to a business or contains discriminatory or racially intolerant remarks – remember unlimited scope for re-publication in social media.

If there is to be an extended or expanded use of the content then Defence should obtain talent and property releases of people and property appearing in content.

Defence must be careful not to directly encourage breaking of the law via its engagement mechanics.

Defence must obey its own published Engagement Principles.

Suggested Engagement Principles to be published to the community that seeks to engage with Defence are as follows:

If applicable, convey rules around use of Defence trade and service marks and iconic defence related images by individuals (e.g. the rising sun badge or the Army logo).

To avoid copyright infringements set clear rules about not using commercial content (unless Defence has a licence to certain content that individuals may access and use for the purposes of the particular engagement).

To avoid copyright infringements set clear rules around not using any form of content unless the content was entirely created by the individual or is being used with the express permission of the content owner. This must apply to all elements in the content including for example any music that is playing as background to audio-visual content.

Provide content rules applicable to the engagement and expressly state that Defence is able to remove content in its discretion.

No uploading of content that contains images of third parties unless the uploader has permission from persons appearing in content or would otherwise expect due to the relationship that their image would be shared in social media.

Provide behaviour rules and codes of conduct to be observed during content creation.

Outline any applicable safety issues and guidelines.

Clearly deal with the question of who owns the intellectual property rights in any user-generated content posting. If Defence will own the content then this should be stated, otherwise it should be clear that Defence is granted a licence to use the content for the intended purpose and any other future intended purpose.

To avoid intermediary liability have an obvious and functional complaint and take down mechanism to provide a channel for third party complaints around privacy, copyright infringement, trade mark infringement, defamation, falsehoods and discrimination.

Provide disclosures and disclaimers around any links to third party sites existing on the Defence site.

Have very clear upfront 'opt-in' consents and disclosures around future electronic and physical communication with the individual if the intent of the campaign is to build or expand a database of individuals interested in Defence - this will ensure best practice Spam Act and Privacy Act compliance.

Have a comprehensive and easy to understand APP compliant privacy policy that is readily accessible at the point of engagement that clearly explains the purpose of collection of personal information and how it will be used in the future.

If Defence is establishing a blog on its own website then it should establish an appropriate code of conduct for contributors, addressing for example:

- who the code applies to and when it applies;
- copyright ownership in posts and ability to maintain and re-post the posts as required;
- general 'netiquette';
- outlawing personal attacks and defamation;
- outlawing unacceptable / inappropriate content;
- outlawing racism, sexism, ageism and religious intolerance and vilification;
- rules on inappropriate and foul language (swearing);
- rules on identifying or referring to third parties;
- rules on providing personal information that may lead to identifying the individual and third parties; and
- outlawing illegal content and activities.

The Engagement Principles outlined above are by no means exhaustive and are provided as a suggested checklist that Defence may consider when it engages in Professional Use of social media and invites or allows the uploading of any form of user-generated content. The Engagement Principles may have general application or may be created for a specific social media engagement activity or promotion.

It is most important that Engagement Principles are clearly brought to the attention of individuals at the point of engagement with Defence via the social media channel. If the rules are only available via an obscure hyperlink or buried in fine print it is unlikely that they will be read by most users and Defence's ability to rely upon them thrown into doubt. Best practice is for the rules to be 'accepted' by ticking a check box (or similar) before being allowed to participate.

Social media policies

a Social Media Policy may govern how Defence and its members engage with the outside community and with each other during Professional Use and Private Use. Such a policy is a conscious effort to inform members about what is appropriate behaviour in social media.

The objective of a Social Media Policy is to set parameters on the use of social media, whether as part of a member's professional responsibilities or in a personal capacity and to limit the risk of damage being caused to Defence and members arising out of such use.

A properly drafted and enforced Defence policy on the use of social media by members is Defence's most effective risk management tool in protecting itself against legal liability and harm to its reputation from the use of social media in during both Professional Use and Private Use.

Some general considerations in creating and implementing a social media use policy include:

- Stressing the ownership and ability to monitor Defence networks and systems and related equipment and explaining that privacy cannot be expected with the usage of such systems. The Federal Court has confirmed in **Griffiths v Rose** [2011] FCA 30 that the monitoring by a government department of its employees' personal use of IT systems will not constitute an invasion of privacy provided employees are informed that such scrutiny will occur. However, the policies do have to be broad enough to cover the types of personal information that may be collected.

- The level of tolerance for personal use of social media by members during work times.

- How members will be trained once the policy is in place so that the intent of the policy can be explained and practised consistently by all members.

- Remind members to familiarise themselves with their terms of employment and all other applicable Defence policies and instructions.

- State that the policy applies to multi-media, social networking websites, blogs and wikis for both Professional Use and Private Use.

- Social media postings should not disclose any information that is not allowed by other policies and instructions, is confidential or proprietary to Defence or to any third party that has disclosed information to Defence, including the personal information of other Defence members.

- In Private Use Defence members should neither claim nor imply that they are speaking on the Defence's behalf.

If a member comments on any aspect of Defence during Private Use they should clearly identify themselves as a member and include a disclaimer. The disclaimer may be as simple as: ‘the views expressed are mine alone and do not necessarily reflect the views of Defence.’

Social media postings should not include Defence logos or trade marks unless permission is asked for and granted.

Social media postings must respect copyright, privacy, defamation, trade mark, consumer protection and other applicable laws.

Defence will need to authorise specific members and approve member communications upon Defence blogs, Facebook pages, Twitter accounts, YouTube channels etc. for Professional Use.

Defence will need to ensure that the Defence records management policy is followed where Commonwealth records are created during Professional Use of social media.

Defence should reserve the right to request that certain subjects are avoided, and request that members withdraw certain posts and remove inappropriate comments as a result of Private Use when the interests of Defence and a member’s employment are involved.

Consider repercussions for policy violations for both Professional Use and Private Use of social media.

Ensure the policy is able to respond to the ever changing social media landscape. As required update the policy so that it remains relevant and ensure members are made aware of any changes. Additional training may be required.

Defence will of course need to consider its own unique requirements when developing a social media policy. Regard must be had to the extant Defence-specific laws, regulations, policies and guidelines that will shape and inform the content of a policy. Further, the laws and regulations discussed in this overview will also influence the policy and the outcomes Defence is seeking to achieve.

It would seem that there are two approaches to creating a social media policy. One approach is to prepare an all-inclusive policy that addresses all currently available social mediums or policies can be created that are specific to each social media network that are used for Professional Use and currently by members during Private Use. Different social media channels have different implications for Defence. Either way, a social media policy should contain some key ingredients and the following is a suggested list of issues that may form part of a policy:

Scope - who the policy applies to and how is it incorporated.

Definition – what is social media (as applicable to Defence) and list the forms it may take.

Consequences for failure to comply.

Contact – to report any inappropriate use of social media.

Clearly distinguish between Professional Use and Private Use of social media.

For Professional Use of social media:

- Only those authorised to comment may do so as a representative of the Defence;
- Explain process of authorisation;
- Follow Defence records management policy for Commonwealth records;
- Set out what can and cannot be done, for example:
 - disclose you are an employee/contractor of Defence, and use only your own identity, or an approved official account or avatar;
 - disclose and comment only on information classified as public domain information;
 - ensure that all content published is accurate and not misleading and complies with all relevant Defence policies;
 - ensure you are not the first to make an announcement (unless specifically given permission to do so);
 - comment only on your area of expertise and authority;
 - ensure comments are respectful of the community in which you are interacting online; and
 - adhere to the Terms of Use of the relevant social media platform/site, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws, and other Defence policies and guidelines.
- If you are authorised to comment as a Defence representative, you must not:
 - post or respond to material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a Court suppression order, or is otherwise unlawful;
 - use or disclose any confidential or secure information; and
 - make any comment or post any material that might otherwise cause damage to the reputation of Defence or bring it into disrepute.
- Set out a moderation policy and approval processes.
- Provide a frequently asked questions section.
- Provide examples of acceptable and unacceptable social media communications.

For Private Use of social media:

- Have a separate set of guidelines (best practice).
- Do not restrict use but encourage best practice behaviour.
- Provide a frequently asked questions section.
- Provide examples of acceptable and unacceptable social media communications.
- For example, state that members must:
 - take responsibility for what they post and exercise good judgment and commonsense;
 - only disclose and discuss publicly available information;
 - ensure that all content published is accurate and not misleading and complies with all relevant Defence policies;
 - expressly state on all postings (identifying you as a Defence member) the stated views are your own and are not those of the department or the government;
 - provide the suggested disclaimer;
 - be polite and respectful to all people you interact with;
 - adhere to Defence equity and diversity policy; and
 - adhere to the Terms of Use of the relevant social media platform/site, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws, and other Defence policies and guidelines.
- For example state that members must not:
 - post material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a Court suppression order, or is otherwise unlawful;
 - imply that you are authorised to speak as a representative

of Defence or the government, nor give the impression that the views you express are those of the department or the government;

- use their Defence email address or any Defence or government logos or insignia;
- use the identity or likeness of another member or contractor of Defence;
- use or disclose any confidential information or personal information of others obtained in your capacity as Defence member; or
- make any comment or post any material that might otherwise cause damage to the reputation of Defence or bring it into disrepute.

Set out what is reasonable/unreasonable Private Use and give examples.

Refer to privacy, confidentiality and information security in accordance with extant Defence policies and guidelines, including equity and diversity.

Address copyright and defamation issues.

Include a reference to all related Defence policies and guidelines.

CLOSING OBSERVATIONS

It can be seen from the topics discussed in this overview that the existing coalition of Australian laws and regulations have a broad application in social media, and are likely in some way to influence and restrict social media engagement for Professional Use and Private Use.

Defence and particularly its members need to understand that laws do apply to social media and members should be educated in their application and trained in what is appropriate social media conduct during both Professional Use and Private Use. Common misconceptions and attitudes towards social media use will need to be carefully identified and adjusted. It is likely that this will involve a review of extant Defence policies and guidelines coupled with the implementation of appropriate Engagement Principles and particular Social Media Policies reinforced by appropriate social media awareness training to engender a culture of obligation to Defence and personal responsibility within members. As indicated above, Defence will need to carefully examine and accommodate the impact of social media upon equity and diversity and its auditing, recordkeeping and disclosure obligations. Such an approach will reduce the legal and reputational risks that Defence will face in social media engagement.

Particularly during social media engagement for Professional Use, the very nature of social media – its collaboration, sharing and conversations – make it all the more important that truth and trust become guiding principles for communications upon and engagement within social media. Interaction with individuals and organisations including the personal

information that is collected and its use should always be permission based. Trust is the currency of social media.

Compliance with the laws and adherence to applicable approaches and risk treatment strategies will not only prevent breaches of the law and adverse publicity, but will assist in establishing and maintaining an appropriate reputation that pervades the social media space.

Stephen von Muenster LLB (Hons) LLM (Media, Communication & IT Law) Principal

VON MUENSTER Solicitors & Attorneys

19 July 2011

ANALYSIS AND INSIGHTS

This section examines Defence practices and attitudes to social media, and international best practice, through the three important ‘pillars’: *management*, *morale* and *marketing*. The three pillars inform and influence Defence in all its other activities, and are just as relevant to the use of social media.

3.1 MANAGEMENT

Social media management is about implementing policy that governs the organisation’s social media activities. In international best practice for armed forces, it includes the daily coordination of efforts informed by general policy and security, but applied to social media platforms.

3.1.1 International best practice

Policy

International military policy specific to social media is in its infancy, as most countries have begun to consider the phenomenon only in the past few years. Documentation provided for this review shows that many policies governing social media in military organisations were written to control the general use of online (or cyber) technologies. The policies refer to ‘cyber’ resources and encompass all aspects of digital communication and collective information sharing.

The evolution of international military policy in this area is most obvious in the extensive documentation provided by the United States, in particular the US Navy. The documents record the evolution of US social media from 2008 and include some plans that address the issue through to 2012. In the material provided, it is not always clear what can be considered policy, as the early stages of policy development involve slightly less formal governance. This section includes examples from material that may have been used to develop policy, or which temporarily stood in for formal policy.

From 2009 to 2011, when formal education and policy were implemented for cybertechnologies and social media, ‘directive-type memorandums’ (DTMs) and guide documents were used in conjunction with governing policies such as those devoted to the US Uniform Code of Military Justice (UCMJ) and OPSEC. The United States opened up the floodgates in 2009 when it allowed the use of social media across all military services, before social media education and policy were fully developed and implemented. Other countries took a more cautious approach, slowly opening up access to certain social media spaces, in order to allow policy to catch up with activity. Each country has had to customise its social media approach, based on its own unique obligations and existing policies.

Documentation provided by the US Navy and other international military organisations covers the key areas of policy development, including:

- structure and roles
- research and planning
- writing and implementing policy
- education.

Documents from all military organisations repeatedly emphasised that social media policy is in its early stages of development and will continue to evolve and grow with knowledge and the invention of new technology.

Vision documents include guiding principles such as ‘Build a little; test a lot’ and ‘Missions drive requirements’ (US Navy 2010a:12). These top-level ideas are considered throughout the research, planning, writing and implementation of policy in the US Navy and other international military organisations.

“We are in the midst of a national dialogue at the moment regarding how we protect both our networks and, at the same time, protect our civil liberties. I don’t think that dialogue has concluded, and I would expect in the years ahead a greater clarity of thought and precision in the development of additional laws and policies.”

(Jack Dorsett, Deputy CNO Department of the Navy Chief Information Officer, 2010c:2)

Table 3.1 shows milestones in the progress of US cyber and social media policy.

Year	Initiative/summary	Milestones
2007	The first military accounts appear in social media.	US Army starts first social media accounts on Flickr, Facebook and YouTube.
2008	Barack Obama’s election as President of the United States is credited significantly to the use of social media, which was legitimised as a serious way for governments to communicate.	Barack Obama is called the first ‘social media President’, as his campaign used social media extensively to create engagement and feed content into broadcast media.
2009	‘We’ve burned the boats ...’ (J Dorsett, pers. comm., 17 December 2009). Phrase used to stress the general urgency of moving forward into the cyber and social media space.	‘Chief Naval Officer’s (CNO) sense of urgency is acute’ (Dorsett 2009a) – the idea that the US should be the leader in technology, not playing catch-up. <ul style="list-style-type: none"> • Strategic roadmap and mission-focused roadmaps. • Directive-type memorandum to open up social media access to all military forces. • Governed by existing policies such as UCMJ and OPSEC. • Objectives for 2011 – senior officer training, IDC (Information Domination Corps) education strategy, cyber workforce, billet realignment (Dorsett 2009a).

2010	<p>The year of planning. Official strategy and draft policy start to emerge, along with the beginnings of an organisational structure that is designed to evolve with the progress of social media in the military.</p>	<ul style="list-style-type: none"> • Strategy planning and draft policy writing. • Organisational structures decided. • Assigned SM roles to staff. • Centralise cyber management activities. • Educational procedures in place. • Initiatives include command/milestone screening board, IDC roadshows and personnel, Intelligence Manpower Distribution Plan, and an IDC Warfare Officer Personal Qualification Standard, Examination and Qualification Process etc. (Dorsett 2010a:1). • Training and education initiatives. • Strike Warfare Intelligence Analyst Course. • Navy Special Operations Maritime Intelligence Training, Center for Naval Intelligence Cyber Curriculum. • Center for Information Dominance. • New IT A School. • NMITC Cyber Curriculum. • Identified F11 Challenges and opportunities • Forward planning strategies put in place (Dorsett 2010a:3–4).
2011	<p>Year of implementation and trial. More official activities begin.</p> <p>First official 'cyber curriculum' begins.</p>	<ul style="list-style-type: none"> • Naval Postgraduate School Cyber Curriculum started by two students in March 2011 (Dorsett 2011a). • Army fake account accusation. • Permanent cyber commander appointed for Navy. Notice of Rear Admiral Kendall Card being promoted to Vice Admiral to serve as the Deputy Chief of Naval Operations for Information Dominance (N2/N6) and Director of Intelligence. Promoted by President Obama; has to be confirmed by the Senate (Dorsett 2011b). • Initial versions of roadmaps published (Dorsett 2011a:3). • Significant budget increase approved for 2012 (Dorsett 2011a:3).
2012	<p>Increased resourcing of social media activity</p>	<ul style="list-style-type: none"> • Budget increase for cyber initiatives (Dorsett 2011a:3). • Focus is on improved integration.

Table 3.1: Milestones in United States cyber and social media policy

Research and planning

US Navy policy has been written and implemented taking into account the vision of the Deputy Chief Naval Officer (CNO) and his superior commanders, including the President of the United States (Figure 3.1).

In May 2010, the Deputy CNO said the US Navy's vision for 'information dominance' was to 'pioneer, field and employ game-changing capabilities to ensure Information Dominance over adversaries and Decision Superiority for commanders, operational forces and the nation' (US Navy 2010a:2). In a 2009 memorandum, he repeated a message introduced by Admiral Roughead in a speech at the Center for Strategic and International Studies (Dorsett 2009a), which was originally spoken by Hernan Cortes at Vera Cruz to show his determination to his troops, 'We've burned the boats; there's no going back'.

This message of urgency meant that the initial research and planning stage was limited. The determination to push forward quickly outweighed the need for involved processes of research, planning and implementation. The Deputy CNO said [W]e must embrace innovation, be willing to test and evaluate new concepts, and ultimately, resource and support game-changing technologies, processes and information capabilities. Our goal: to achieve command and control overmatch against all adversaries' (Dorsett 2009b).

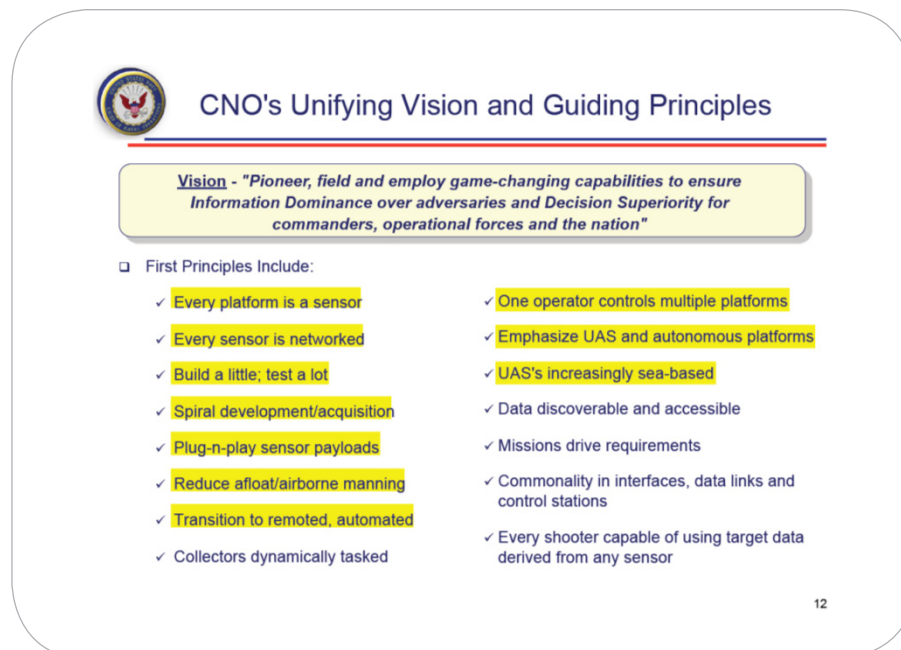


Figure 3.1: CNO's unifying vision and guiding principles

(Source: US Navy 2010b:12)

Civil liberties and the desire for military dominance have driven policy development in the United States, and that must be considered when making comparisons with Australia. Visions, principles, goals and objectives feature prominently in the documents. Detailed presentations and educational material focus on toplevel cyberinitiatives, which are then applied to social media policy planning.

Despite warnings from the US Department of Defense (US DOD) that ‘social media amplifies risk due to greater volume and increased speed of information shared publicly’ (US Navy 2010c:2), the Army and Navy opted to go ahead with substantial social media activity before the completion of policy. They were able to bypass the process by following the spirit of other policies and upholding the core values of the organisation in social media.

The Navy focuses on defence first and foremost, and justifies the aggressive launch into social media by the use of a cyber-rule designed to structure approaches to general cybersecurity breaches. Called the ‘85% rule’ (Leigher 2011), it refers to the percentage of problems that can be managed through standard Navy network security. Strategy and tactics are only developed for 15% of problems in cyberspace generally, and that policy can be applied comfortably to social media. Policy is needed to cover the 15% of problems that are not covered by standard Navy network security. The interpretation could be that OPSEC covers 85% of problems that may occur in social media and that only 15% of situations need specific policies, generally for the interpretation of existing policy on social media.

Canada provided a document based on academic research that examines the effects of new media in a military environment (Parsons 2010). It looks at new media and society, social change produced by new media and the effects of social media on an operational military environment. The document highlights the complexity of separating social media from the wider subject of digital communication by showing how each segment of new media is connected to another.

Social media policy research analysed in Canada includes an examination of the social science behind the identity beliefs of individuals and how they evolve over time. Social identity research can provide insight into the behaviour of individuals and groups, and shows how offline patterns are often mimicked in online environments. In writing policy to govern the behaviour of individuals in a social environment, it can be beneficial to understand what drives the target audience to use and engage in social media in the first place. As Upal (2010:iii) argues:

“Understanding how people’s social identity beliefs evolve over time and in response to information that people encounter in their daily lives is important if we are to build a predictive model of social influence that could be used by the Canadian Forces, since identity conflicts are thought to underlie many of the current and future conflicts around the globe.”

Canada is looking at the social science behind the forming of communities and what drives behaviour in order to formulate an overall cyber-approach, using social media as an important tool to implement the results of the research. A practical understanding of areas such as identity conflict, identity performance and identity politics can be achieved through engaging with and monitoring an audience in social media.

Roles and responsibilities

In the US Navy, the first phases of policy development involved establishing the Information Dominance Corps (IDC), with the mission of assisting all fleets to complete their missions through cyber-resources. However, in addition to specific, detailed areas of policy, there are also more general principles that guide the longer term strategy. The US Chief of Naval Operations, Gary Roughead, regularly emphasises the importance of utilising resources across a range of platforms (Figure 3.2), which is why the IDC was formed as its own fleet.

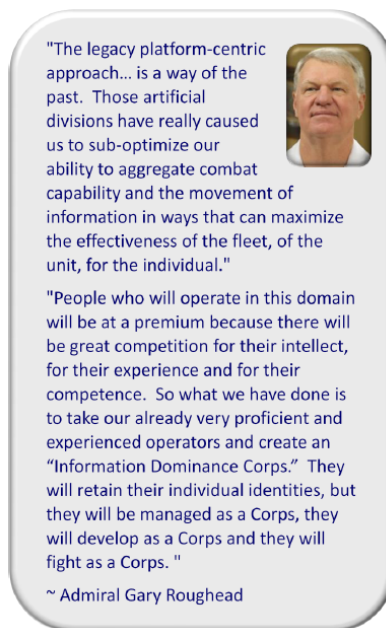


Figure 3.2: Admiral Gary Roughead on information dominance
(Source: Dorsett 2010b)

The US Navy then implemented an organisational structure with roles and responsibilities for commands (Sullivan and Kutch 2009). Commanders such as the CNO were formally given the responsibility of educating personnel and assigning social media management roles (Dorsett 2010b:1) necessary to carry out the command social media or cyberstrategy, or reassigning that task to another suitably qualified military professional. The IDC includes personnel from a range of military roles, including civilians, enlisted personnel, junior officers, mid-grade officers and senior officers (Dorsett 2010b). Around 45,000 military personnel are in information management roles (US Navy 2010b:14).

The US Army has a similar process for the delegation of responsibilities. Its public material is targeted more specifically to social media, as opposed to the general cyberstructure approach of the Navy. The first step is a DTM delegating the responsibility for management of the 'electronic online presence' to all Army commands (McHugh 2009). The document then permits the Army Command to reassign that responsibility to a qualified general officer. This DTM is the first formal step in the longer term creation of official governing policy for structure and roles.

Writing and implementing policy

The common theme in the writing and implementing of policy internationally is the utilisation of existing policy. Policy for social media should be kept to a minimum to avoid conflict and confusion with other policies. Jack Dorsett advised the IDC that using existing policies across multiple departments and platforms is preferable to having individual policies for each unit (Dorsett 2009a). New policy should not contradict or compromise principles included in the UCMJ and OPSEC and can generally be written by adapting or updating an existing policy.

The US DOD echoes the same sentiment, pointing out that all actions taken by Air Force members are subject to the UCMJ first and foremost (US Air Force 2009); other, more specific policies required for social media work within the framework of the UCMJ. Social media may be considered communications and entertainment tools that all US military personnel are entitled to access, but the US DOD stresses that they 'now fight wars on multiple fronts; one of which is the information front' (US Air Force 2009:2).

The US DOD aims to achieve 'centralized new media policy – decentralised execution' (US DOD 2010a), which can explain why most policy material relates to the interpretation of existing policy to cater for new media. This is achieved through presentations and guides addressing specific issues such as posting images to Flickr (US Army 2010a) and how to write tweets (US Army 2010b). The US Air Force guide (2009) states that 'this guide does not advocate a major shift in resources from traditional media to new media. Rather it endorses the belief that digital communication provides a new toolset that commanders can use to achieve military objectives.'

The Canadian Forces have found a way to attempt to implement social media policy through terms and conditions of use, which are published on their website. This means that the policy governing the Canadian Forces member in an online space is clearly published in an online location. The official terms encourage personnel to consider the potential risk to themselves and others if they post certain content online and to consult with their command before posting potentially sensitive material (Canadian Forces 2011).

Education

A significant volume of policy documentation provided to this review was about education and training. The documents indicate that programs, initiatives, seminars and resources are made available to military personnel internationally, in addition to policy and guidelines.

In 2009, planning began on US top-level social media policy. Most activity centred on education on how to interpret social media in the light of existing policy. In the United States, education is based on both the toplevel cyberinitiatives and specific social media initiatives; the US Navy focuses its attention on the former and the US Army focuses on the latter.

Quarterly memos are distributed to the IDC from the Deputy CNO, Jack Dorsett, summarising the activities undertaken by the IDC in the areas of cyberinitiatives and education. In October 2010, strategy behind the Intelligence Manpower Distribution Plan inspired training initiatives, including the Strike Warfare Intelligence Analyst Course, Navy Special Operations Maritime Intelligence Training, the Center for Naval Intelligence Cyber Curriculum and the NMITC Cyber Curriculum (Dorsett 2010a). The first two students commenced studying the Naval Postgraduate School Cyber Curriculum in March 2011 (Dorsett 2011a) as the first step in trialling the ongoing cyber-education plan.

The Navy Cyber Forces (CYBERFOR) is the executive agent of these warfare training programs. CYBERFOR's responsibilities include issuing the requirements and procedures for qualification and designation as an 'enlisted information dominance warfare specialist' (EIDWS) (Meek 2010) and other cyber-related roles. The creation and designation of new roles or training programs is communicated through memorandums and official letters to ensure that governing policy is kept consistent. As Meek (2010:1) notes:

*"Individual commands shall designate the Command Master Chief (CMDMC) or Senior Enlisted Leader *(SEL) as the command's EIDWS Program Manager (PM). The EIDWS PM may designate a Program Coordinator to assist in running the day-to-day specifics of the warfare program, but the PM retains the responsibility of running a fair and comprehensive program."*

These training programs are being implemented for the first time, so memorandums outlining relevant policy and procedures in relation to accelerated qualifications (Meek 2010), designations of official information dominance warfare officer status (US Navy 2010d) and authorisation for commanding officers to administer the qualifications for IDC officers (McCullough 2010) are regularly sent between commanding officers. To become information dominance warfare officers, military personnel undertake training to receive appropriate qualifications (McCullough 2010). These memorandums provide useful examples of policy implementation procedures in a social media environment.

Educational material provided by the US Army is more specifically relevant to social media and to the existing OPSEC policies, so that material has been covered in the 'OPSEC' section below. The material is in the form of guides and 'how to' documents for specific social media services such as Facebook, Twitter and Flickr. This education is delivered through seminars and presentations, and printed and digital material is available for both military personnel and their families. Subjects covered include how to post images, how to avoid OPSEC breaches and other logistical implementation factors related to the individual software platforms and how they work together with existing policy.

Records management

The use and adaptation of existing policy have created extensive challenges in the area of record keeping, for which few best practice examples are available internationally. There is confusion about how to define official and unofficial correspondence in social media, and how to identify valuable or important content that should be archived.

Initially, the US Army suggested that 'some effective means of archiving information include ensuring the content posted on social presences is also available via a command website, archiving email related to command social presences, taking screen captures of social presences and copying and posting content into a text file or Word document' (US Navy 2010e:9), which would create extensive work for social media managers.

In an effort to reduce this resource requirement, the Army released a document related to Web 2.0 use and record value that 'provides a basis for determining whether federal records created using web 2.0 tools should be retained for a temporary period of time or are permanent and ultimately transferred to the National Archives' (NARA 2010:4).

‘Official content’ is deemed to be any outgoing communication that comes from an official channel, but ‘social media’ is not clearly defined as an official or unofficial channel, leaving the record-keeping decisions up to the individual commands. Whether internet posts are official or unofficial currently depends on where they are posted and by whom; policies are flexible (NARA 2010) and evolving, as with all other social media policy.

The simplest interpretation of international record-keeping policy is that all outgoing communication should be housed on an official website that provides both a credible source for the community and a method of archiving content. The content can then be shared easily into social media, and important or significant conversations can be selected for archiving.

OPSEC

OPSEC is at the heart of global military operations and management and has important implications for the use of social media. Internationally, operational cybersecurity in military organisations aims to educate military personnel and their close community, such as friends and family, on the importance of maintaining awareness of potential risks when discussing military information in social media, publicly or privately.

Generally, OPSEC in military organisations is not communicated as a set of rules but rather as general strategies to deny enemies access to information (OSPA 2011). In the US material, the term ‘enemy’ is used to describe any individual or group that may be using information to endanger the safety of military personnel or the community.

OPSEC strategies are communicated as a range of educational material and programs that aim to assist departments, individuals and families to navigate social media in a military environment. Examples of OPSEC materials and case studies in the next two sections (OPSEC for families and OPSEC for military personnel) highlight the importance of education for military personnel and their families. The US DOD is used as the primary exemplar of best practice in this area.

Case study: The Robin Sage experiment

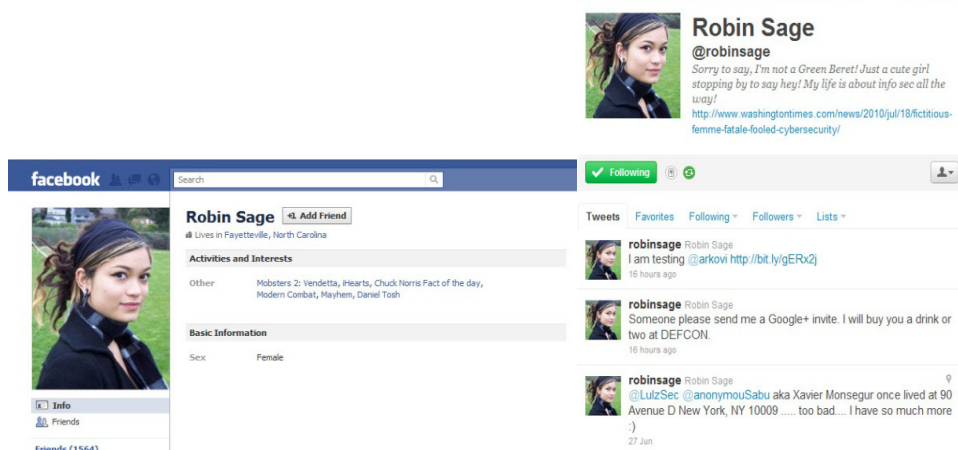
Who: Fabricated person Robin Sage, US Department of Defense and Thomas Ryan

Where: United States of America

When: December 2009

What: 28-day experiment using online social media accounts for 'Robin Sage' to demonstrate how cyberthreat analysts could be fooled in the United States

How: Facebook, Twitter, LinkedIn



Facebook account

Twitter account

Cybersecurity company Provide Security used the Robin Sage experiment to demonstrate the 'outflow of information as a result of people's haphazard and unquestioned trust'. The lead person of the experiment, Thomas Ryan, set up multiple social media accounts in the name of 'Robin Sage', creating the online persona of a female cyberthreat analyst, and began 'friending' and 'connecting' with other cyberthreat analysts in social media. By 'joining networks, registering on mailing lists and listing false credentials', Ryan used Robin Sage to research the decisions of those connected to 'trust' and share with Sage. People who connected with Sage included executives from the National Security Agency, the US DOD and Military Intelligence groups. Over the course of the 28day experiment, Sage received job offers from government and corporate entities and invitations to speak at conferences, and was offered gifts. Information revealed to Sage from connections 'violated OPSEC and PERSEC procedures', although that may have been a result of the tactical choice to create Sage as a female in an industry that is dominated by males. Ryan's decision to make Sage a young, attractive female brought an interesting response from some of the male connections, who offered jobs and tickets to conferences and complimented Sage about her pictures. Ryan states that the 'worst compromises of operational security I had were troops discussing their locations and what time helicopters were taking off.'

Sources: Ryan (2010), Fabrizio (2010).

OPSEC for families

In the United States, it is deemed important for the entire military community to be educated about the requirements of OPSEC. This includes parents, partners and children living on and off base. Seminars and other communications channels (such as social media) are used to present educational material outlining the potential dangers of using social media, which may not have been considered by those who do not receive complete military training.

OPSEC educational material for families focuses on:

- instilling pride in family members by letting them know they are as much a part of the military community as their 'soldier' (military representative), with their own responsibilities for keeping the soldier safe
- providing guidelines to help them avoid inadvertently revealing information to enemies by discussing seemingly unimportant details publicly in social media
- providing examples of attempts by enemies to gather intelligence on soldiers using family activity in social media such as Facebook, Twitter and blogs.

OPSEC for families, including educational materials, is underpinned by the values in Figure 3.3. The US DOD references the Operations Security Professional's Association's *OPSEC for families* educational material, which focuses on simplified key points with general values to teach family members how to make decisions in social media. It stresses that information is a jigsaw puzzle and that any piece, no matter how small, can endanger lives (OSPA 2011).

OPSEC guiding principles

- 'Denying enemies access to information'
- 'OPSEC is a way of thinking, not a set of rules'
- 'Always assume that the enemy is reading what you're writing'

(Operations Security Professional's Association 2011)

Figure 3.3: OPSEC guiding principles

Mitigating misuse

In documentation provided to families by the US DOD (US Navy 2010f), OPSEC is introduced as a strategy, rather than a set of rules. The family member is assigned an important role in the protection of military personnel. Pride and security are used as primary drivers to inspire family members 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.

An example of this educational material (Figure 3.4) shows how fear is used as an educational driver. The material features an alleged appeal from alQaeda to its members to seek out information about the family, state of origin and rank of US military personnel. This example is used to illustrate how simple details acquired by the enemy may be used against US soldiers.



Figure 3.4: Example of US Department of Defense training material
(Source: US Navy 2010f:3)

The British Ministry of Defence gives clear instructions to commanders about considering what is shared online (BMD 2011a). As well, commanders are responsible for speaking to friends and family about their responsibilities when it comes to the sharing of information. Documentation explicitly instructs military personnel to inform friends and family of what can and cannot be posted online.

The overwhelming majority of material reviewed in relation to this subject focuses on education as a way of mitigating misuse of social media. The educational process includes military personnel and the community that surrounds them, generally using positive drivers such as pride to encourage cooperation, although some fear tactics are also used.

Responding to misuse

Generally, publicly available documents about responding to misuse of social media in the armed forces provide clear and comprehensive steps to be taken. However, it is difficult to report the consequences without compromising the privacy of the military personnel involved.

In the US Army, social media managers are advised to contact individuals who are breaching the guidelines, but to do so in a casual manner with an educational goal (US Army 2011). It advises social media managers to contact individuals who have breached OPSEC and ask them to remove their posts themselves, rather than doing it for them and risking offending or censoring the individual (US Army 2011).

The approach with families is positive, educational and inspiring in the first instance, but limited information was made available about ramifications if a family member continues to breach guidelines.

Harnessing for branding

Family members are not openly discouraged from discussing military matters, which may promote the positive brand of the services. However, they are not provided with specific guidelines in this area. Rather, military organisations attempt to create Facebook pages and blogs with content that family members can engage with, publicly showing the positive relationships between the forces and military families. The family member is ideally engaged with the content in a positive way, which would be evident to their friends in social media and therefore promote the service as a positive community with which to be involved.

The US Army outlines the importance of allowing and encouraging social media communication within the organisation and the wider community, referring to this activity as a 'mission essential' (US Army 2010c:3) partly because it builds positive morale among military personnel. Family members contribute to social media, build websites and comment on blogs, and those behaviours help to promote the positive ideology that drives US military organisations.

Meeting public obligations

The educational processes for families and the community help the forces meet their public obligations for privacy, security, freedom of speech and public disclosure. However, challenges with record keeping and accessibility in relation to third-party services exist across all areas of social media internationally, and all reviewed countries are involved in ongoing attempts to manage them.

As channels to communicate information to the public, social media help to meet the public's expectation that they will be informed of how US military organisations are engaged. As well, they provide avenues for the engagement of family and friends and opportunities for those groups to be heard by the organisations that employ their sons and daughters.

Family readiness groups

Official and unofficial online family communities exist in a variety of social media, including Facebook pages and groups, blogs, forums and websites. These online communities, aimed at family members of military personnel, are referred to as 'family readiness groups' (FRGs) (US Navy 2010b:9). The following are examples of FRGs from the United States.

NAVYforMoms.com and NavyDads.com (unofficial)

- Builds morale through connection between members and military personnel.
- Supports security through regular inclusion of OPSEC guidelines as content (that is, blog posts).
- Photos, stories and personal experiences contribute to positive branding and organisational pride.
- Uses content provided by OPSEC in website terms of service and guidelines.
- Self-moderating community with shared values and a goal of protection.
- Social media network functionality, such as connecting to friends, sharing photos, posting to forums, reading and commenting on blogs and publishing events.



Source: <http://www.navyformoms.com/>

Source: <http://www.navydads.com/groups>

OPSEC for defence personnel

In contrast to OPSEC for families, OPSEC for military personnel focuses more on the interpretation of general military rules and guidelines in a social media environment. US military organisations attempt to relate all online activities back to the overall governance of defence personnel, in particular by referring to the UCMJ (Air University 1950) using specific digital examples.

Educational material for the management of Defence personnel focuses on:

- the interpretation of existing military codes in a digital/online environment or software solution
- procedures for the delegation of management responsibilities to commanders and their subordinates
- guidelines for general decision-making processes, with example scenarios
- the implementation of policy, responsibilities and procedures and education about them in specific commands.

Mitigating misuse

The US DOD attempts to mitigate misuse of social media by military personnel through a tiered process of education and responsibility. A social media guide for Air Force personnel states that 'it is up to the Public Affairs professionals at each level to teach and enforce Air Force new media policy, by training and educating every Airman on the proper use and techniques of engaging in social media' (US Air Force 2009:7).

Defence personnel are provided with training that uses educational materials (for example, US Navy 2010a, 2010b), some of which are also made publicly available. The material focuses on the basics of social media use and includes tips such as the following:

- Separate personal and professional social media accounts (note that this conflicts with the policies of social networks such as Facebook, which allows only one account per user).
- Report abuse to your commander and to the social media service if necessary.
- Username and password combinations to avoid.
- Be extra wary of strangers and check connection requests thoroughly.
- Engage openly under the guidelines of OPSEC.
- If in doubt, refer to top-level policies.

In addition to educational material made available to all military personnel, innovative services such as the Virus Hotline (Department of State 2009:11) connect military personnel instantly with the Virus Incident Response Team, which can assist with security compromises in real time.

Misuse of social media can be defined as actions that may endanger any military personnel or their families, in addition to the security of any mission, present or future. The US DOD recommends looking for the following common misuses when monitoring social media:

- Service members or family sharing too much information.
- Posts about scheduled movements or current or future locations of ships/units.
- Detailed personal information (employer, position etc.) (US Navy 2010g)

Responding to misuse

International best practice puts each command in charge of its own social media presence. Managers are assigned the responsibility of monitoring military personnel under their command, or delegating that duty officially to one of their team members.

Managers in the armed forces of the United States and United Kingdom are instructed to identify and remove information that may compromise military security (US Navy 2010g), while the New Zealand Defence Communications Group recommends contacting the person and using the incident as an opportunity to educate them, at least in the first instance (M Crane, pers. comm., 20 June 2011).

The US Army states that leaders 'should respond in the same manner they would if they witnessed the infraction in any other environment' (US Army 2011:5). However, this general instruction does not clarify how it is to be interpreted in a digital environment.

The British Ministry of Defence (2011b) offers a helpful guide to what to do if something goes wrong online. It accepts that individuals will inadvertently make mistakes in social media as guidelines are clarified and technology continues to change rapidly, so it uses guidelines based on examples to guide personnel on what is expected of their behaviour.

The US Navy has also produced a general operational risk management (ORM) process (Figure 3.5), which is another guiding set of ideas and steps to assist military personnel in making the right decisions in a generally unpredictable environment. It is intended to be used not just in combat but also in cyberwarfare, as it is believed to be general enough in application to govern all situations that might arise.

Operational Risk Management

- **Five step ORM process**
 1. Identify hazards
 2. Assess the hazards
 3. Make risk decisions
 4. Implement controls
 5. Supervise and watch for change
- **Applying the ORM process to scenarios (examples)**
 - Angry comments on blog
 - Information leaks through social network
 - Israeli mission cancelled
 - Sailors killed in Afghanistan – personal

Figure 3.5: Operational risk management
(Source: US Navy 2010h)

Harnessing for branding

The role of military personnel in marketing is no longer a passive one. Internationally, personnel are encouraged, not simply permitted, to engage in social media and promote the positive aspects of their job to the greater community.

The US DOD tells its airmen that:

- *while communication with media and the public has traditionally been the responsibility of Public Affairs, today all Airmen are communicators ...*
- *all airmen are encouraged to use new and social media to communicate about topics within their areas of expertise, or their interests*

(US Air Force 2009:1)

This is guided by the idea that 'If the Air Force doesn't tell its own story, someone else will' (US Air Force 2009:1), which is echoed internationally in documents supplied by the various defence forces.

The Air Force needs to turn all of its Airmen, and especially its front-line Public Affairs specialists, into communicators who combat the negative influence of enemy propaganda, misinformation and misrepresentation. We are training world-class Airmen to act as our communicators who can successfully wage an information media war against our detractors. (US Air Force 2009:5)

Encouraging engagement can raise challenging questions, such as how to allow military personnel the freedom to express themselves while maintaining the positive brand message of the organisation. The US DOD instructs personnel to 'replace error with fact, not argument', in an attempt to avoid inaccurate messages that may result from online arguments (US Air Force 2009:5).

The following case study gives an example of how the Department of Defense harnesses social media to enhance its brand.

Case study – Getting started with blogging

Who: US Department of Defense
Where: United States of America
When: 2010
What: Guide to creating official pages on behalf of DoD
How: SlideShare, blogs

US DoD realised that to leverage its brand in social media it needed to empower and equip its personnel to create blogs that aligned with the brand. To do this, it provided a guide to setting up blog presences that covered the following topics:

- Why blog?
- Things to think about (generally)
- Tips for successful blogging
- Terms of use
- Blog moderation
- Measuring blog effectiveness
- How to handle guest comments
- Further resources.

The guide is not just a step-by-step guide to setting up a blog. It addresses the strategic and tactical issues associated with presenting the US DOD brand, including goal setting, planning, marketing, and developing processes for maintaining the blog once it is established.

‘Blogs put a human face on the embassy or consulate and create an engaged connection with people in the host country.’

Source: US DOD (2010b).

3.1.2 Defence practices and attitudes

Over six weeks, this review examined Defence’s current mix of policies, processes and overall engagement in social media channels to develop a robust understanding of how Defence manages social media. The review team also conducted over 26 hours of one-on-one interviews with Defence personnel to gain a greater understanding of not only the current perceptions of social media within Defence, but also how specific personnel use social media in an official capacity for engaging either the public or personnel in their organisation.

This section outlines the key areas of focus: strategic direction; policy setting; education and training; and ongoing management and monitoring (Figure 3.6).

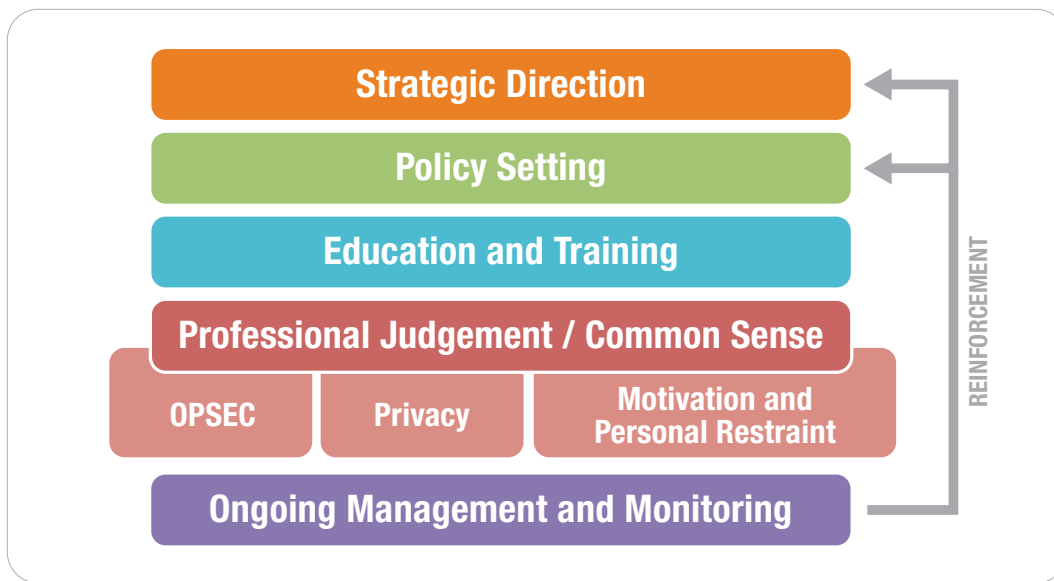


Figure 3.6: Critical elements in Defence's approach to social media

Each of the four factors plays a critical role in Defence's current approach to social media. Overall, the interrelationships between a number of organisational facets have resulted in approaches to and perceptions of social media that are somewhat fragmented.

Strategic direction

The review team examined existing Defence documentation on social media and interviewed a wide array of individuals to understand their perceptions of this emerging phenomenon. Indeed, new sources of information on Defence's current social media activities continued to be identified up to the end of the review period, so this report is by no means exhaustive. Early on, it became clear that Defence has small pockets of social media innovation.

Jacka and Scott (2011:26) argue that:

"Experimenting is okay and most likely the best way to start, so long as everyone understands that these are experiments (or it could be viewed as a series of incremental successes and failures). It doesn't mean that the activities should not be aligned with the business objectives, but just that there might be less formality to the overall function in terms of scope and resources. In some ways, organizations that are hesitant to engage in social media might be best served by a series of small but focused tests to determine to what extent these activities should become a permanent part of the business operations."

Although the 'test and learn' approach to social media has been used by Defence thus far, the main purpose has been to leverage social media channels for external marketing and communications by approved members of Defence, relying on existing media policy.

Defence's social media practices have been developed and tested by lower and mid-level employees, with a focus on very specific and tactical execution for external marketing and communication purposes. During this review, it became clear that the general Defence approach to the 'why and how' of social media can be used is still in its infancy. As a result, it can be inferred that the test and learn approach to innovation within the Services has yet to produce a consistent high-level approach to developing the channels further. In contrast, the US military organisations initiated their massive policy and strategy changes as a result of a presidential decree, to ensure that members would not have their constitutional rights to freedom of speech infringed or curtailed by overrestrictive policies.

Opinion: Joint Force Quarterly, National Defense University Press, Quarter 1, 2011

The natural reaction of many commanders may be to assign one staff section as the proponent for social media, leaving the responsibility for integration to them. While that approach may be easier to implement than some of the other options, the risk is the social media program will become viewed as a niche program and will not get the attention it might deserve. Furthermore, the social media program would assume the natural biases of the assigned staff element, decreasing its broad effectiveness. For example, if J6 (Command, Control, Communications, and Computer Systems staff section) were the proponent, it might input a technical bias, and likewise the Public Affairs (PA) section might tend to approach social media as an outreach tool only. Thus, broad integration may provide the best opportunity to achieve the results desired.

(Mayfield 2011:81–82)

Executive sponsorship and strategy development

Although small teams in Defence have been testing social media, there are inconsistent practices within and between Defence organisations trying to understand the channels and assess the opportunities and risks of using them in an official capacity. Previous business case submissions for social media monitoring and online metric tools have allegedly been rejected because small teams were primarily responsible for all costs and there was no opportunity to centralise expenditure and deliver this service to all teams currently engaging in this field. Due to the lack of centralised strategy development and visible executive sponsorship, a strategic assessment of social media channels, including cost–benefit analysis, has yet to be conducted. A more thorough assessment is required to identify how to operationalise social media from a human and technological resourcing perspective.

The absence of consistent sponsorship for social media across Defence means that there are both an opportunity and a need to establish 'ownership' and ultimately take a much more robust and holistic approach to social media that aligns it with Defence's overall strategic objectives.

Resourcing

Many employees using social media as part of their jobs within Defence have been given those responsibilities in addition to their regular workloads. Moreover, while some are extremely progressive and are primarily self-taught and self-motivated, others have been handed the responsibility with limited knowledge and appear to be struggling to motivate themselves to maintain the incremental workload.

Staff turnover within command structures has been relatively high (as has been the case among those who have accepted or been given responsibility for social media). As a result, momentum for developing channels within Defence has been inconsistent. Additionally, some social media roles have been left vacant for long periods, which has resulted in an on/off approach to using social media.

Some Defence employees (including those who are in the Australian Public Service) are managing social media outside regular working hours. They recognise that, because of the instantaneous nature of posts, moderation of the channels cannot be confined to office hours.

The review team endeavoured to identify personnel throughout Defence who currently have responsibilities for the ongoing management of social media pages deemed 'official' by the organisation. The team's social media audit identified a number of other pages and accounts that could not be confirmed as either official or endorsed by Defence. The review was unable to conclude whether there were any resourcing commitments for the unconfirmed pages.

The level of innovation, content, responsiveness and overall engagement in some of the social media presences has merit and should be seen as a direct reflection of not only the individuals managing the presences on a daily basis, but the strategic leadership, endorsement and direction from within the broader Defence organisation, although that support is fragmented at this stage.

Service strategy development

Currently, each Service independently manages its own policies and procedures for the use of social media. Previously, the teams managing official social media for the Services had established a support network, in conjunction with the Department of Defence Communication and Media Branch, to share knowledge. However, due to the resourcing problems referred to above and reassignments of members, the support group has largely disbanded. Resourcing shortfalls have resulted in some Defence social media presences remaining largely inactive for almost a year.

Throughout the interviews, it was widely acknowledged that the Navy social media team is currently the most active and engaged in the space, although both the Army and the Air Force are active on their official pages (see the audit results in Section 2.3).

Navy social media guidelines

In addition to Defence policies, the Navy has established social media guidelines targeted at Navy personnel and more detailed guidelines for individuals responsible for the development of content and interacting online. The current Navy guidelines, many of which rely on best practice in the United States, cover the following areas:

- *Social media explained*
- *Who uses social media?*
- *Social media in the Navy*
- *Guidelines for using social media in the Navy*
 - *Operational security*
 - *Protection of your families*
 - *Membership in military-related social groups*
 - *Online interactions and behaviour*
 - *Avoiding the violation of trademarks and copyright*
 - *Understand profile security settings.*

Additional guidelines have been established for individuals with online and social media content responsibilities to ensure that content being published on behalf of the Navy is in line with offline media guidelines. The guidelines address the components listed above, but in more detail for content creators. The additional subsections include the following:

1. *Make Navy proud, make Australia proud – Always express ideas and opinions in a respectful manner*
 - a. *Make sure your communications are in good taste.*
 - b. *Be sensitive about what content you link to. Redirecting to another site may imply an endorsement of its content.*
 - c. *Do not denigrate or insult others.*
2. *Be yourself and transparent*
3. *Be sensible about how much you reveal*
4. *Keep your cool*
5. *Admit mistakes*
6. *Don't be fooled*
7. *Avoid the offensive*
8. *Don't violate privacy*
9. *Avoid endorsements*
10. *No impersonations*
11. *Stay in your part of the ship*
12. *Use common sense*
13. *Safety*

(T Sargeant, pers. comm., 8 June 2011)

The Navy and Army and Facebook terms of use

Both the Navy and the Army have established Facebook page rules and guidelines governing how individuals can post and what types of content can be removed. It is noted by this review that across Defence there are several ongoing initiatives attempting to update or create robust social media guidelines. The following information can be found within the policies:

- *Standard of conversation and the removal of content, which is offensive, inappropriate, or could impact national security or Defence. This includes:*
 - *Graphic, obscene, explicit or racial comments or submissions that are abusive, hateful or intended to defame anyone or any organisation.*
 - *Links to non-government websites, other Facebook groups or posts may be removed at the discretion of the Social Media team.*
 - *Removal of comments that suggest or encourage illegal activity.*
 - *The apolitical nature of the site and posts attacking either side of the Australian Government will be removed.*
- *You participate at your own risk, taking personal responsibility for your comments, your username and any information provided. This page will be monitored regularly to detect any inappropriate behaviour and posts that breach the guidelines. Any posts that do breach the guidelines will be deleted. You should also be aware of what other people can see on your own profile if you haven't restricted access to it.*
- *Spammers or trouble makers will not be tolerated (people whose sole reason for being here is to cause trouble). Your posts will be deleted and you will be banned immediately.*
- *By joining the Australian [service] official Facebook Fan page and using the provided service you agree to the above guidelines.*
- *Also, the appearance of external links (like Facebook ads) on this site does not constitute official endorsement on behalf of the Australian Army nor the Department of Defence.*

In addition to the above Facebook guidelines, Army has also provided the following information:

- *For any recruiting inquiries contact 131901 or visit Defence Force Jobs.*
- *Defence personnel should read DI(G)ADMIN 08-1 before posting anything on social networking sites such as Facebook.*
- *You should also be aware of what other people can see on your own profile if you haven't restricted access to it.*

(Sources: <https://www.facebook.com/RoyalAustralianNavy?sk=info>,
<https://www.facebook.com/TheAustralianArmy?sk=info>, retrieved 22 June 2011)

Air Force Facebook guidelines

The guidelines for participating in the official Air Force Facebook page are somewhat shorter:

“Please note: This is an official Air Force page; therefore, it is essential that a suitable standard of conversation is maintained at all times (i.e. no material is to be provided that could offend, humiliate or intimidate another person, or, if disclosed, has the potential to affect national security or damage the reputation of the RAAF, ADF, Navy, Army, Department of Defence or the Government). This page will be monitored regularly to detect any inappropriate behaviour. You should also be aware of what other people can see on your own profile if you haven’t restricted access to it.”

(Source: <https://www.facebook.com/RoyalAustralianAirForce?sk=info>, retrieved 22 June 2011)

However, the Air Force also provides links to educational material covering participation in social media and targeted at Air Force personnel. The following quote is provided to reinforce posting rules for Defence personnel:

“Defence personnel should read DI(G)ADMIN 08-1 before posting anything on social networking sites such as Facebook.”

(Sources: <http://www.airforce.gov.au/images/FacebookPRF2.pdf> ;

<http://www.airforce.gov.au/images/security-poster.pdf>;

<https://www.facebook.com/RoyalAustralianAirForce>, retrieved 10 July 2011)

Army social media handbook and SOPs

The Army has developed three important documents concerning social media (T Sargeant, pers. comm., 8 June 2011):

- *Army social media handbook*

- *Social media summary*
- *Social media for soldiers and Army personnel*
- *Social media standards for Army leaders*
- *Checklist for OPSEC compliance*
- *Establishing and maintaining an Army social media presence*
- *Using social media in crisis communications*
- *Checklist for setting up a social media presence*
- *Army branding*
- *Australian Army social media case studies*

- *Social media standard operating procedures: Army Headquarters*

- *Regiment/Brigade/Unit*
- *OPSEC*
- *Mitigating risk*
- *Individual/personal use*
- *The threat environment*
- *Categories of personal information: personal information; employment details; operation information*
- *Protecting your information*
- *Protecting your friends' and colleagues' information*
- *If you suspect information has been released in error (escalation process)*

- *Standard operating procedures, Strategic Brand Coordinator, Army Headquarters*

- *Day to day business*
- *Removing material*
- *Weekly reporting*
- *Facebook chats*

iArmy

The Army launched a new intranet site in 2011 which is accessible within the DRN, called iArmy. This site is still within a growth phase and as site access was restricted during this review, the team was unable to assess social media content housed on iArmy during the review period. This platform is considered a priority communications channel for personnel and as such, it is recommended that updates to policies, Army social media guidelines, SOPs and educational material be made accessible through the iArmy intranet.

Joint Operations

Middle East Area of Operations

There is currently a Facebook presence for Joint Task Force 633 which represents Defence's Middle East activities. At the time of this review, the page is listed as a community page, rather than a Government Organisation or Defence/Military page. Moreover the page name is listed only as "Joint Task Force 633" with no reference to Defence which means that it cannot be found within search results unless individuals know the exact title of the page. Finally, the URL for the page is <https://www.facebook.com/AustralianArmyAfghanistan> and does not reference either the Joint Task Force or ADF. These inconsistencies have ultimately limited the reach of JTF 633 content and thus makes it quite challenging for interested stakeholders and the Australian public to find out about the ADF's activities in the Middle East.

This page is promoted primarily to personnel, family and friends of those deployed in the region and journalists. When on deployment, friends, family and media follow JTF633 as a way to track activities in the region. Although this is a Joint Operations page, it has a much lower reach than many of the other social media presences operated by Defence as it does not appear to be promoted to the broader Australian public.

The page is intended to provide an honest communication channel to parties with a vested interest in activities in the region. Currently public affairs officers are responsible for managing the page in addition to headquarters. The page is used primarily as a broadcast mechanism, rather than one for ongoing engagement with the target audience. As such, page administrators do not respond to the same degree as administrators of the top-line official Navy, Army and Air Force pages.

During interviews with Joint Operations personnel, it was acknowledged that the team has modelled its activity after the US Marines.

Talisman Sabre 2011

Throughout the Talisman Sabre exercises in 2011 in Queensland, a joint social media taskforce was set up to manage social media on behalf of both the US Military and the ADF. The social media presences were heavily resourced, to ensure content was updated throughout the day. Both governments had invested a high volume of personnel to the channel to maximise the overall public relations opportunities during this biennial event. As such, there were a significant number of personnel equipped with high quality photographic, video and editing equipment who were scheduled to record the events so they could be posted on social media and made available to journalists in Australia and abroad. Although the end result of Talisman Sabre's social media demonstrated a fantastic use of best practice, Defence cannot underestimate the massive investment by the US and Australia with respect to human resources. These individuals were solely dedicated to this social media initiative and extremely intertwined with Public Affairs and operational logistics.

Insights

Although some joint operations have been established in social media, others such as those in Timor and Solomon Islands have yet to set up a presence. To ensure broad consistency across joint operations, a resourcing model should be considered.

The current Joint Operation social media teams have endeavoured to innovate and identify international best practices and as such, further activities should be aligned with the other official Defence social media channels to maximise the communication benefits.

Policy setting

The primary Defence policy guiding the use of social media is *Public comment and dissemination of official information by Defence personnel (DI(G) ADMIN 08-1)*, which was last issued on 5 October 2007 and last reviewed on 5 October 2010. The policy clearly states:

“Defence personnel must treat official information as confidential. Defence personnel must not provide public comment, official information or images to individuals or organisations external to Defence without adhering to the procedures detailed in this instruction. Public comment and dissemination of official information includes, but is not limited to....video newsletters, ‘home videos’, documentaries, publication of information and imagery on the internet, mobile networks including SMS, email and attachments, and other electronic media, ‘blogs’, ‘chat rooms’, podcasts, text messaging and all forms of ‘new media’. It also includes discussion, personal opinion or correspondence with members of the public on official information.”

The list of digital channels and the open-ended interpretation of ‘new media’ has been used to capture emerging channels, such as Facebook, YouTube and others. Although the policy has been set out to manage official communication by Defence, its broad coverage would prevent Defence personnel discussing any of their professional employment activities on a social networking or media site.

The document contains three other sections (quoted below) that should be considered, as they also have an impact on the use of social media within Defence.

Publication of official information and imagery on the internet, mobile networks and other electronic media

“Official information that is distributed electronically, online or through any form of new media (including ‘blogs’, chat rooms, podcasts and text messaging) is subject to the same coordination, clearance and authorisation requirements as hard copy materials and imagery.

Given the speed and potential breadth of dissemination of material via new media, all Defence personnel must be vigilant in ensuring these procedures are vigorously followed.

No official information may be transmitted or appear online without prior approval and clearance for fact, policy, operation security and sensitivity from the relevant Service Chief or Group Head or their One Star/Band One (or above) delegate and authorisation from DGPA or DGPA’s delegate.

Without prior approval and authorisation, Defence personnel must not engage in public debate in online forums or by other electronic means using official information.”

(Annex D to DI(G) ADMIN 08-1, p. D-4)

Based on the current social media practices within Defence, a more detailed review of the approval processes for all social media posts, comments or moderating procedures should be undertaken. Current practices for each of the Services vary significantly and have been affected by staff turnover and resourcing. Unlike traditional media channels, social media involve extremely short response times and participants demand an almost instantaneous response. Therefore, it is critical to understand the process by which each of the Services, and other affiliated Defence social media channel operators, manage their content.

Many other government departments and many corporations have updated their media policies and procedures to address the specific needs of social media. Among other things, their policies cover:

- the registration and administration of social media sites, with either endorsement by or affiliation to the agency or department
- approval processes and response/moderation procedures for enquiries, general commentary, privacy, and negative or defamatory remarks made on official social media channels
- service-level agreements for managing response times and identifying responses requiring specialist comment
- risk management procedures, including escalation and crisis management – both of which require real-time monitoring to ensure continuity and the identification of issues as soon as they arise
- cross-functional oversight committees to establish and monitor the overall strategic direction of social media and how they will be used as established channels, rather than solely for small tests.

Private communication and non-official communication

DI(G) ADMIN 08-1 refers directly to private communication and non-official communication by those who are not currently deployed overseas:

“When engaging in private online or electronic discourse and transmission of imagery or information, either in Australia or from deployed operations, All Defence personnel must consider the potential impact of that material reaching the public domain.

Defence personnel must use professional judgement to ensure that no information sent privately breaches operational security or adversely affects the safety and wellbeing of Defence personnel and their families, or Defence’s reputation and international relationships.

Defence personnel are not to produce unsanctioned or bogus ‘Defence’ internet sites which can be attributed to them as Defence employees, Defence civilians, or Defence members. Regardless of attribution, official information is not to be included in private or non-official communication.”

(Annex D to DI(G) ADMIN 08-1, p. D-5)

This element of the policy addresses the generic need for OPSEC in addition to the need to protect privacy and the reputation of Defence. However, it is unclear whether individuals who are not deployed are allowed to communicate with others about their jobs or lives as members of Defence in general terms. Moreover, confusion remains about information that is deemed non-official or private in relation to Defence:

Given that Defence tends to be under much more scrutiny than most businesses, and that the separation between personal and Defence business seems to be blurred, especially by the media, then Defence should maintain a more restrictive policy on how social media is employed by its members and provide guidelines as to how that information is accessible. I have no objection to Defence members using social media, but it is the unintended consequences of the sharing that needs to be advertised. A good set of security guidelines for all users should be distributed to all members as a minimum (as per current practice for deployed members, but this should extend to all staff).

(Anonymous response by Defence member)

Certain elements in this part of the policy are quite unclear, not only about social media but also in relation to general communication. For example, if an employee were to 'whinge' about a commanding officer or a colleague to a friend at the pub, or to their partner using email or private communication within social media, would and should that be treated differently from posting a public comment on a social media site? By clearly defining the types of information that fall into the categories of private, official and unofficial, there can be greater clarity and confidence when individuals refer to Defence in general. When these policies were discussed with security professionals within Defence, the simple act of identifying oneself online as a Defence member was considered problematic.

Non-official or personal communication from deployed operations

"Communicating with friends and families back home while deployed on operations has a direct and positive effect on morale and, in return, on operational effectiveness.

A principal consideration in these communications, whether they are by mail, phone, email or the web, is to understand the impact that they can have on Defence's reputation and our international relationships. It is even more important to understand the implications that the careless transmission of classified or private information can have for our operational security and the safety and wellbeing of Defence personnel and their families.

It is only through your sound judgement when communicating your experiences, whether while deployed or in person once you return home, that we can be confident that we are each protecting Operational Security and promoting Defence.

The enduring challenge for all Service men and women has always been to communicate openly with our families and friends while managing these important issues. It is a responsibility that all Defence personnel must take seriously. The following principles assist in meeting this challenge.

Principles

- *Alongside specific communication security measures to protect OPSEC on each operation, all deployed personnel are encouraged to speak with their families and friends only about their specific areas of responsibility.*
- *Defence personnel must always remain conscious of the impact that their communication, whether it be text, audio, images or video, might have on our operational security, the safety and wellbeing of Defence personnel and their families, Defence's reputation, and Australia's international relationships.*
- *Where an incident involving death or injury has occurred, non-official traffic from the operational area may be temporarily suspended to ensure that the next of kin of those most affected are the first to be informed. Defence personnel must specifically avoid identifying the names, units or locations of those injured or killed until such information is publicly released by Defence.*
- *When communication is re-established, Defence personnel must be careful not to speculate on the cause of the incident, or to comment on the incident's details or ongoing processes, or to compromise any current or future inquiry by discussing details that might be legally admissible as evidence.*
- *Where an incident has occurred, eyewitness accounts provided to anyone other than official inquirers must be basic and avoid detail.*
- *Defence personnel are not to comment on the investigative process or aspects that will be subject to the capture of evidence. All Defence personnel must work to ensure that due legal processes are allowed to proceed.*

Blogs, web-based discussion forums and 'new' media

Official information that is distributed electronically, online or through any form of 'new' media (such as 'blogs', chat rooms, text and image messaging) is subject to the same coordination, clearance and authorisation requirements as hard copy materials and imagery. Those requirements are detailed in annex D of this instruction.

Defence personnel must not use official information in online forums or transmit it by other electronic means without prior approval and authorisation.

When engaged in online forums or when sending information privately, Defence personnel must exercise professional judgement to ensure that no information breaches operations security or adversely affects the safety and wellbeing of Defence personnel and their families, or Defence's reputation and international relationships.

(Annex 8 to DI(G) ADMIN 08-1)

One perspective on the elements of an effective social media policy

An effective social media policy includes the following elements to ensure appropriate engagement within social media channels:

- The overall objective of the social networking policy and the organization's approach to social media.
- The pertinent rules that apply to the use of social media throughout the organization.
- The social media boundaries and communications considerations:
 - Who is responsible for postings to the organization's social media—department, titles, and names, if applicable.
 - The employee's role in the organization's social media conversation.
 - The employee's responsibilities and limitations outside their employee/employer relationship.
 - The need for transparency, disclosure, and how to address any conflicts of interest.
 - A description of how to ensure compliance with applicable laws.
- A description of taboo areas and websites that may be blocked.
- A statement on proprietary and confidential materials (including sensitive information about the organization, its customers, and its employees).
- Where to turn in the event problems are identified (especially those that could result in a crisis communications situation).
- Where to turn if employees find they are having problems.
- A connection with the organization's code of conduct and ethics guidelines.
- Guidelines related to all types of media (video, music, etc.), not just the written word.

(Jacka and Scott 2011:93)

Although there are a significant number of heightened restrictions for personnel deployed overseas, those based in Australia should not take for granted anything related to the OPSEC, personal privacy and reputational impacts of social media. By reviewing the entire *DI(G) ADMIN 08-1* policy document, Defence can reduce contradictory or confusing elements involving the use of social media and communication in general. The policy should be consistent across all platforms, whether it covers phone, face-to-face, email or social media communications.

Implications for Defence policy

As mentioned above, *DI(G) ADMIN 08-1* requires updating to ensure clarity of roles and responsibilities in social media, specifically for official Defence social media channels, but also for private communications about Defence activities in social media. However, updated policy also needs to link appropriately to the policy on protective security in relation to the Chief Security Officer's activities for audit, conformance and accountability.

In addition, appropriate updates should be made to *DI(G) ADMIN 10-6 Use of Defence telephone and computer resources* to ensure that personnel using social media in an official capacity use it in an appropriate way. Finally, a review of whether specific social media sites may be used for personal matters using Defence assets (especially for those on deployment) in order to support morale should be undertaken. An initial assessment of social media channels by the Department of Defence Command, Control, Communications and Intelligence Division (Defence Science and Technology Organisation), titled *Don't judge a (Face)book by its cover: a critical review of the implications of social networking sites*, has been completed. The assessment was only recently published, in May 2011, so it will be critical to ensure that Defence feedback about it is incorporated into further policy and process updates.

Operational security

'There is a need for greater understanding of the security implications of the information posted in social media pages. I see too many members who post info/pics of themselves which identify that they are service personnel and what unit they belong too and where they are serving on operations. There also needs to be greater awareness that info posted on the Internet is there forever and that no matter how secure the site is, there are people who will find ways to access it.'

(Anonymous response by Defence member)

Although predeployment OPSEC training has a significant social media component, many members of Defence do not believe they have been given any training in social media. The quantitative social media survey of Defence personnel asked, 'Have you been trained/briefed on the use of social media?'; only 42% personnel answered 'Yes'. These results are concerning, as the current policy relies on personnel to use 'common sense' and 'professional judgement' but leaves them to interpret those terms subjectively.

Privacy

Privacy in social media has been the subject of much attention over the past few years. Although the media have largely focused on the privacy settings of social media sites such as Facebook, additional factors need to be considered. Many individuals who use social media are extremely trusting and have connected with friends not seen since primary school, or with people with whom they have had little or no interaction, such as someone they met at a party. Throughout the qualitative interviews for this review, some interviewees said they had taken steps to protect their identities online, but many had not even thought about the issue. Most did not recognise that people using fake profiles, perhaps masquerading as school friends, could capture information and movements.

Although some respondents were driven to lock down their profiles as a result of their career aspirations (such as a role in Special Operations), many others did not. During the interviews at ADFA, for example, the cadets who were most concerned about privacy online had learned about protecting their identity from relatives or friends, rather than from ADFA training material (Figure 3.7).

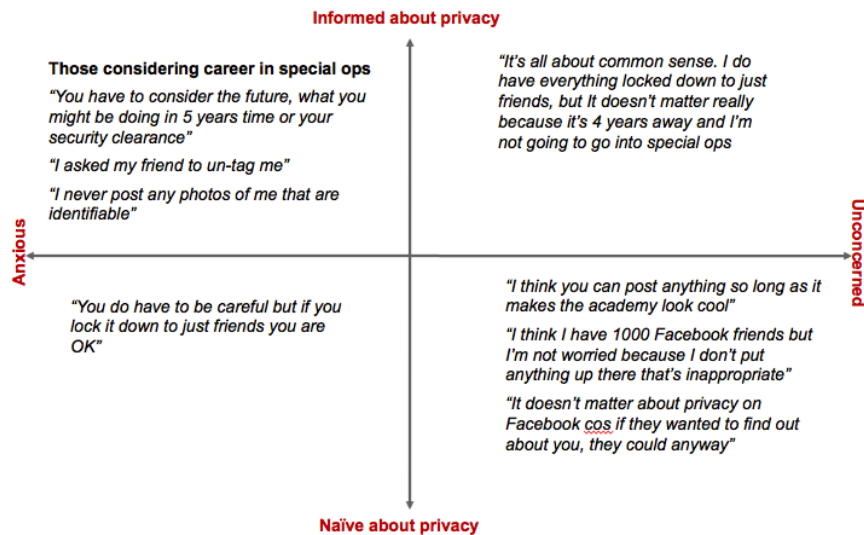


Figure 3.7: ADFA respondents' views on privacy

For some individuals within Defence, avoiding scandal is more important than other privacy considerations, such as privacy settings, who they choose to connect with, or what other information is shared. Few consider the possibilities of data mining and how patterns of behaviour can be identified over time. This is especially true for some of the cadets at ADFA, who do not recognise or acknowledge that information could easily be gleaned from posts to establish a behavioural profile that could be used in a negative way. In addition, due to the intensity of the ADFA program, many of the cadets tend to share information such as parade ground temperatures, plans for the evening, jokes and general cadet gossip. They often operate within a bubble, and some largely ignore the fact that their broader 'friends' networks can see into their ADFA Facebook world.

However, the ADFA cadets also demonstrated a deep and lasting desire to protect their brand and not bring Defence or their Service into disrepute. They showed pride in Defence, their Service and themselves as individuals, as well as disapproval of those who seek to tarnish the Defence reputation. There are also compelling signs that many cadets understand mitigation processes: some referred to the process of organising or

reorganising their social media affairs before attending ADFA, including by reducing the number of online friends and limiting access to their profile. While there is sometimes a gap between the actions of some cadets and their pride and personal values as Defence personnel, there does not seem to be a culture of rejection of Defence values. However, their inexperience and trust in social media were reflected in their poor understanding and acceptance of how and by whom activities and content in those media will be received.

Research demonstrates that overt reliance on social media privacy settings has also led to a false sense of security. Despite having stringent security settings, many individuals reported having more than 300 friends on channels such as Facebook.

Motivation and personal restraint

“Young people do not understand that things that are put out into the social media can not be taken back this has the potential to be harmful to defence any posting of any thing defence related should be vetted to stop the wrong information getting out and any offenders be dealt with as required.”

(Anonymous response by Defence member)

“Defence must consider security when using Social Media, also the Now attitude of its younger members wanting to share with friends and not realising that once something is out there you can't get it back.”

(Anonymous response by Defence member)

Although the responses quoted above show heightened concern among Defence personnel about younger personnel and cadets sharing information, Defence must also recognise that the younger cadets entering the armed forces are from a generation of what have been called ‘digital natives’. Marc Prensky coined the term in 2001 to describe people who have grown up using email, internet connections and various forms of social media and other online tools. For them, those methods of communicating are perceived as entirely natural and commonplace (Prensky 2001:1).

For some, the phenomenon can be confronting and challenging. In many organisations today (as in the general community), this can sometimes lead to conflicting views about the use and utility of the media. One respondent to the review survey stated:

“Defence should completely ban the use of any form of social media. Defence should retrain personnel in the use of a pen, paper and postage stamp. I cannot think of anything worse than to spend as much time as I already have to on a computer, to then go and spend more time on one just to socialise.”

While not all personnel hold such views, some do. Both opinions need to be respected in an effort to give social media its rightful, but balanced, place in Defence.

Common sense

One of the main phrases that stand out in OPSEC training materials is ‘professional judgement’, which is used interchangeably with both ‘sound judgement’ and ‘common sense’. Moreover, the current *DI(G) ADMIN 08-1* does not explicitly define or mention ‘social media’; nor does it fully explain the available channels, beyond a rudimentary list. The result is that personnel have to make decisions about how, when and why they use social media (both officially and unofficially), informed by ‘common sense’, using ‘sound’ and ‘professional judgement’.

Indeed, based on research conducted during this review, there is significant misunderstanding of the role of social media and how service men and women should be using them. Many of the responses to the quantitative survey indicate that training in social media is inconsistent and has not necessarily resonated the way it was meant to. Despite efforts to encapsulate social media in both policy and training materials, there is still much confusion, and the terms ‘professional judgement’, ‘sound judgement’ and ‘common sense’ are subject to widely varying personal interpretation. This results in systemic risk in the use of social media within Defence.

Although the focus of this review is on social media, it has found that personnel will express themselves in other ways outside social media, such as in the creation of the ‘Stiff Sh*t Books’, while on deployment. One respondent to the survey stated that they were concerned about:

*‘... the fact that unacceptable/adverse or perceive unacceptable/adverse media/communication could lead the individual(s), organisation, command to face lawful judgement and or litigation. This is supported due to what I have seen throughout my career concerning the use of the old ‘Stiff Sh*t Book’ on ships, graffiti and email. Electronic communication is very difficult to govern or control.’*

Although social media bring a new set of risks, many of the factors that could damage the Defence reputation have always existed. They are just being manifested in different ways.

Although Defence can block access to social media sites via Defence ICT assets, a complete prohibition might simply move potential problems to nonDefence systems. With the explosive growth of personal smartphones and tablets, it is highly likely that Defence personnel will use social media while deployed. By providing the appropriate policies, education and monitoring tools, Defence can effectively reduce the level of risk associated with sites such as Facebook.

Divergent attitudes across Defence

During the quantitative study, more than 900 free text responses were submitted by Defence personnel in response to the question, ‘How should Defence manage social media differently to civilian businesses?’ The following five quotes demonstrate how the culture and appreciations of social media’s benefits and risks are inconsistent across the organisation:

“There should be NO social networking networks available to ADF members. ADF members should be discouraged from using social networking sites, as ‘Pattern of Life’ monitoring is standard within intelligence collection. These networks present a clear and present danger in relation to potential security leaks.”

“Defence should establish guidelines for the use of social media. This should be included within Defence Security Manual and other official security publications. All security training should be adapted to educate/inform members of the potential dangers associated with Social Networking media.”

“Defence should allow easier access to certain social media but have a set guideline so that users don’t give away what they may doing, i.e. deployments, exercises etc., as this would get a better picture of what is happening in the greater Defence community as well as a good recruiting tool to be used in the future.”

“Social Media is a new medium that needs to be assessed and analysed. It is becoming more and more mainstream and Defence needs to get on board but not with old draconian rules that do not fully apply to the new medium. Defence needs to manage and train all staff to manage their interaction and exposure appropriately. For instance, [in regards to] Facebook I have the highest possible privacy codes applied and do not divulge my work, or where I live, or location. This allows me to socialise with family and friends appropriately. Twitter, I use as a more open medium and therefore do not post photos, locations or anything about me personally. I have however seen relatives who are in the Australian army who post photos and locations and details of what they do for all to see on Facebook. I consider this inappropriate use of Facebook by Defence personnel.”

“Social media plays an important role in daily lives of many people, defence needs to adapt to the world with social media prevalent on every corner, however at the same time the nature of our business will require us to have stronger and stricter control over our exposure in the social media.”

The challenge for Defence is that common sense and professional judgement cannot be seen as purely objective when the opinions of personnel vary so much. This results in difficulties when issues of policy endorsement and enforcement are considered. To mitigate social media risks, Defence leadership needs to establish a clear strategic direction for the use of social media and update policies routinely.

Education and training

Defence is no different from other organisations whose personnel have to contend with increasingly complex policies, procedures and protocols. The only way to ensure that policy is understood is through targeted education and training. However, 53% of Defence personnel surveyed do not believe they have ever received social media training from the organisation, and another 5% are unsure. These results mean that Defence cannot assume that the current policy on social media has been understood, or even read, by most personnel.

Training for cadets

The appropriate use of social media by ADFA cadets is addressed very early in their induction process. There is a focus on common sense and the do's and don'ts of social media in order to avoid scandal, or bringing ADFA or Defence into disrepute. In the survey carried out for this review, the cadets mostly focused on the following points to protect against risks:

- No identifiable photos of bad behaviour.
- Pictures in uniform only if behaving appropriately.
- No photos with guns, Rambo-style.
- No negative references to ADFA or Defence.

Cadets recalled the following quotes from their social media training induction at ADFA:

“Give it the 60 second test before you post it up on Facebook.”

“They say to imagine what it would be like if it was on Today Tonight.”

“If it was on the front page of the paper, what would you think about it?”

Many of the cadets appreciated that they were being given personal responsibility, without ADFA being too prescriptive about the use of social media. They were consistent in their concerns about bringing the program into disrepute. When a negative situation arises in social media, it might be seen as the action of an individual using poor judgement, rather than an attempt to circumvent an order. As one cadet commented, 'We all wanted to know what we could and couldn't put [on Facebook] and they basically said anything that made ADF look cool was good.'

Comments such as that indicate that directions might not be specific enough and remain open to individual interpretation. This can lead to inconsistencies in how cadets understand the term 'common sense'. The strong focus on the reputation of ADFA masks broader issues of identity and privacy, which cadets do not seem to understand well.

Training for Defence personnel

Predeployment briefings on OPSEC are currently the main way Defence personnel are educated about risks in the use of social media. The learning objectives that address social media in those sessions are as follows:

- *ICT security – Working on Defence networks (DRN/DSN) and what can be stored on those networks; using non-approved wireless/LAN connections for personal computers; nonapproved video calling and information capture devices (thumb drives, PDAs) and attachments to social networking sites.*
- *Information security*
 - *Disclosure of activities and location via email.*
 - *Utilise veiled speech when communicating with family.*
 - *Defence personnel must not use official information in online forums or transmit it by other electronic means without prior approval and authorisation.*
- *Incidents involving death or VSI.*
 - *Avoid using names, locations or speculation around incident in order to avoid compromising the privacy of affected families or investigations.*
- *Social media and hand-held imagery*
 - *Revealing the location of Defence personnel may present a personal, family and/or operational security risk.*
 - *Establishes patterns of behaviour.*
 - *Geo-tagging of photographs enables enemies to identify specific locations.*
 - *Smart phones embed geo-tagging in SMS messages.*
 - *Guidance for disabling automatic geo-tagging on social media and hand-held devices.*

- *Personal security*

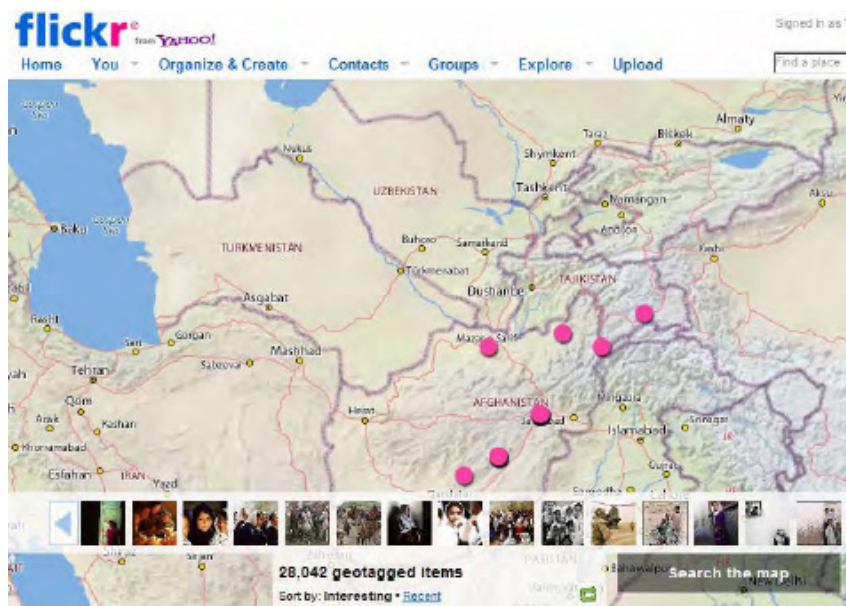
- *Activate personal security measures.*
- *Consider who are added as friends.*
- *Consider advising family of your FB content.*
- *Consider providing site passwords to your next of kin.*
- *Uniforms in personnel photos make you a target.*
- *Unintended disclosure – friends and family may unintentionally disclose sensitive information.*
- *Generation gap – what you think is acceptable in your peer group or within your demographic can be deemed in poor taste, culturally insensitive, racist or prejudicial by commanders or the public.*
- *Fake profiles – media personnel and enemies create fake profiles to gather information. For example, the Taliban have used pictures of attractive women as the front of their Facebook profiles and have befriended soldiers.*

(Source: MEAO Force Preparation Training – OPSEC Brief, 39th Personnel Support Battalion)

The quantitative survey for this review revealed inconsistency in the provision of training. OPSEC briefings were the main channel for training, followed by annual security briefings and briefings by commanding officers and security officers, but other channels were also used. The primary sources of educational information were OPSEC training guides. Many individuals stated that the training was relatively ad hoc – another potential source of inconsistency. In addition, as a result of the diversity of opinions held by Defence personnel, it is likely that some members were told not to use social media, while others were educated about how to use it.

As a short-term measure, it would be beneficial to develop a concise version of the OPSEC training guide for social media, which could then be used for induction and refresher training for nondeployed personnel. However, the training materials would need to be updated routinely to take into account any changes in policy.

The Army OPSEC briefing for 39th Personnel Support Battalion demonstrates tangible and realistic examples of the risks that social media use poses to personnel. Although some of the examples are specific to Defence, the training officers have also used real-world examples from other sources to ensure that the message is well understood.



The following was published in Wired magazine in 2009

I ran a little experiment. On a sunny Saturday, I spotted a woman in Golden Gate Park taking photos with an iPhone. Because iPhones embed geodata into photos that users upload to Flickr or Picasa, iPhone shots can be automatically placed on a map. At home I searched the Flickr map, and scored – a shot from today. I opened the user’s photostream and determined it was the same woman. By adjusting the settings to only show her shots on the map, I saw a cluster of images in one location. Clicking on them revealed photos of an apartment interior—a bedroom, a kitchen, a filthy living room. Now I know where she lives.

(MEAO Force Preparation Training – OPSEC Brief,
39th Personnel Support Battalion, received 16 June 2011)

Enforcement and monitoring

The use of social media within the defence force opens up a whole can of worms when it comes to operational, personnel and physical security. Until defence can introduce measures to monitor and put in place rigorous SOPs on how social media applications can be used by members of the DOD and Public Service, the use of such systems need to be barred for use on all Defence establishments/sites, operational deployments and places of work. The improper use of social media applications by members of the defence force has already had implications for the ADF and created negative public/press comment towards the ADF."

(Anonymous response by Defence member)

"If the recent homophobic Facebook page incident had happened within a civilian workplace (e.g. McDonalds) I have no doubt that the employees who openly aligned themselves with the view espoused on the 'No Gay Maccas Employees' page would have been disciplined and more than likely fired almost immediately, and yet within defence that is not the case. We should hold ourselves to a higher level of accountability, not lower. And we should be more specific in our training to remind people that Facebook is NOT private, and it IS permanent. There should be very clear and explicit regulations regarding social media use and they should be reinforced through education and enforced through the discipline system."

(Anonymous response by Defence member)

Those in direct command of personnel are required to address any misuse of social media, but only the more serious instances of misuse are fully documented. Therefore, it is not possible for this review to assess the volume or frequency of such incidents.

Defence's approach to misuse might reasonably be based on the concept of providing an educative rather than a purely punitive response – something encouraged by other armed forces assessed in this review. Such an approach would be consistent with that taken to most 'everyday' matters of enforcement of military policies and guidelines.

Interviews showed that the consequences for social media 'misdemeanours' are variable – sometimes nothing is said and sometimes the offender suffers major repercussions. This inconsistency might result from a lack of appreciation of the potential risks of misuse, meaning that poor behaviour is recognised only during more serious infractions, which end up being reported either in the traditional media or by someone in a social media friendship group. Personnel responsible for enforcing policy should receive incremental training and advice about what constitutes bad behaviour online and how to reprimand personnel for infractions, consistent with other Defence practices.

Overall, feedback from personnel supports the view that monitoring social media practices and enforcing social media policy need to be priorities for Defence. The current lack of monitoring tools to measure and moderate Defence's online channels, and the limited human resources available to manage the channels, are risks that need to be considered.

EMAIL HIGHLIGHTS FROM DCOORD-A, OFFICE OF THE CHIEF OF ARMY

SUBJECT: USE OF SOCIAL MEDIA TO SUPPORT UNIT COMMAND

TO: COMMANDING OFFICERS

DATE: 20 APRIL 2010

SECURITY

You must be aware of the intent of the DI(A) 55-2 (attached), which, written before social media took off, still lags in written guidance on what is acceptable or not in social media. The DI(G) is being rewritten for release in Oct 2010. In short keep to the principle that what you say or do as an individual on Facebook not only brings your own image into question but what you say in in your role representing Army and the Government should be carefully scrutinised because it can bring the wider organisation's image into focus. You might also consider SEN Faulkner's commitment to a more open Defence Force but understand also the potential damage a slip can make when transmitted to 13,500 people instantly ...

CONCLUSION

The development of social media as a tool for supporting the chain of command has been embraced by the US, well in advance of Australia, and is already actively supporting both US Army and USMC corporate and unit communication. Where used wisely social media is likely to provide Army with an agile and flexible means of communicating messages and coordinating support and importantly, listening to what our soldiers and families want to say.

Government 2.0

The attitudinal survey of Defence personnel demonstrates the broad range of opinions about security and reputation in social media. As the scope of this project was limited to understanding social media use by Defence personnel, the review team did not address broader questions about personal security and personal and organisational reputation outside the social media context. However, it is clear that a number of individuals will be highly resistant to embracing these channels of communication. Leadership from the top will be needed to overcome these challenges.

According to the government's response to the report of the Government 2.0 Taskforce (2010:3):

The Australian Government is committed to the principles of openness and transparency in Government, and a Declaration of Open Government is an important affirmation of leadership in these principles. A Declaration, in conjunction with the Australian Government's proposed reforms to the Freedom of Information Act 1982, will also assist in driving a pro-disclosure culture across government.

The Government 2.0 response is closely aligned with two critical elements within, "Ahead of the Game: Blueprint for the Reform of Australian Government Administration." The two focus areas within the document for the Australian Public Service (APS) include creating a more open government and improving engagement with citizens.

The government's focus on transparency is underpinned by the use of Web 2.0 and social media technologies. Its response to the taskforce's report goes on to state (p. 5):

“Agency activity implementing Web 2.0 technologies into their everyday business practices will be important if the government is to embed Government 2.0 cultural change in agencies.” (Government Response to the Report of the Government 2.0 Taskforce, 5).

Centrally coordinating Defence's high-level social media strategy would facilitate the development of cost-benefit analyses and funding and resourcing models. As the Government 2.0 response states (p. 6):

The cost of agency change required to address internal technical and policy barriers will be the responsibility of agencies to absorb as part of their business-as-usual activities. Finance will create an online forum to assist agencies to record their initiatives and lessons learned.

The proposed Digital Executive Oversight Committee (DEOC) will benefit from working with the Department of Finance and Deregulation (the lead agency for Government 2.0) to understand detailed management practices in other government agencies.

To overcome internal resistance to change in social media use, the Government 2.0 response states (p. 7):

Australian Government agencies should therefore enable a culture that gives their staff opportunity to experiment and develop new opportunities for online engagement ... Agencies should also consider that a broad range of stakeholder groups are considered for engagement online.

A number of Defence personnel have demonstrated innovation and leadership in the social media space, and they should be acknowledged for their work thus far. Acknowledging those efforts can help to highlight the benefits of change and overcome some of the negative stigma associated with the channels.

In line with the Government 2.0 Taskforce's Recommendation 10: Security and Web 2.0, the lead agency is to liaise with Defence Signals Directorate to develop a better practice guide for the use of Web 2.0 tools and update the *Information security manual*. Moreover, the Information Commissioner is to address this when developing guidelines under freedom of information legislation. DEOC should take direction from the lead agency to ensure that all social media development is aligned with broader government obligations in relation to the *Freedom of Information 1982* and the *Archives Act 1983*.

Record keeping and archiving

Because the National Archives of Australia (NAA) considers social media to simply be channels in which Commonwealth records can be shared, existing record management and archiving protocols need to be followed. The challenge lies in identifying Commonwealth records worthy of archiving but also in the resourcing and processes required to ensure compliance. The government's response to the Government 2.0 Taskforce (p. 15) states explicitly that the Archives will produce guidance on what constitutes a Commonwealth record in the context of social media. The NAA should be consulted to provide greater clarification for DEOC.

3.1.3 Discussion

Internationally, social media have been embraced as one way for governments and military organisations to communicate with stakeholders. The international military community has considered the risks and concluded that it is necessary to be 'part of the conversation'.

Defence is likely to see real benefits from implementing a revised social media policy. The policy review might consider establishing DEOC and an official social media adviser role to clarify the overall strategic direction for administering the use of social media. Sponsorship at an executive level would ensure that current and future social media initiatives are consistent with Defence's overall strategic goals. Because the needs of the different Services vary, social media administration will still need to be considered within the individual Services.

However, as the international analysis has shown, an overall policy direction based on recognition of the place social media might play within Defence would be beneficial. *DI(G) ADMIN 081 Public comment and dissemination of official information by Defence personnel* and other similar policies (which may not have come to light in the review) will need to be reviewed to incorporate updated sections about social media, or a separate social media policy will need to be established. New policy developed for social media will be more effective if it does not conflict with other existing policy, guidelines or Defence values.

Any overall strategy and policy direction would need to take into account local legislation and culture. A 'one size fits all' approach, simply adopting what has been implemented elsewhere, might have limitations. While the US has adopted a liberal approach with a strong emphasis on freedom of speech, a more centralised control of social media presences might work more effectively in Australia, instead of attempting to explicitly empower all military personnel to represent the Defence brands and commands.

Because social media use results in an overlap of personal and professional activity, the policy should address that overlap by providing clear guidelines about acceptable use during personal time, which would apply whether on base, in Defence housing or when deployed. Personal use guidelines should apply in all locations, as social media can be accessed almost anywhere in the world.

The review of international best practice and Defence practice in Australia shows that, currently, the primary reason for educating people about the use of social media is to support OPSEC.

OPSEC is heavily reinforced with Defence personnel before and during deployment. However, threats to security created by sharing information in social media can never be ignored, regardless of whether a person is based in Australia or overseas. Family members and the wider community have the potential to put Defence members and themselves inadvertently at risk through their use of social media. Knowledge of social media privacy issues varies widely within the community, and that variance is reflected in the survey responses of cadets at ADFA. The review team acknowledges that peer advice in Defence social media communities already exists and has helped to limit security breaches and damage to the Defence brand.

For professional uses of social media, the review team recommends that Defence review the social media access restrictions on the Defence Restricted Network to ensure alignment with the longer term social media strategy to be developed by DEOC. The scope of work for this review explicitly deemed security analysis of social media use to be out of scope, as the review team is not specialised in risk management and Defence security protocols. Detailed security implications should be addressed by Defence personnel in the next phase of social media strategy development.

The use of appropriate educational materials and their reinforcement can significantly reduce the risk from the misuse of social media. Those materials should be consistent about what is expected of Defence personnel, and should rely much less on subjective terms such as 'common sense'.

After strategy and policy have been adjusted, current social media educational and briefing materials should be reviewed.

Defence may wish to consider formal training for relevant personnel, which could include:

- a basic understanding of the tools of social media
- realistic and practical social media guidelines that match the policy
- the identification of processes for Defence social media channel administrators
- risk management protocols for identifying social media problems early and strategies to deal with them, whether or not they have escalated in importance.

As with occupational health and safety training, it would be beneficial for social media training to be reinforced annually. The training would be in addition to all predeployment OPSEC briefings, as repeated reinforcement will help to ensure that social media use works with and complements the goals of Defence.

Finally, tools to support the understanding and management of social media should be implemented to supersede current monitoring, which is manual, inconsistent and narrowly focused. They could potentially include metric tools to measure online activity and engagement and moderating tools to flag inappropriate content posted online. For such tools to be used effectively, Defence requires specialised personnel to resource and monitor the media, so intervention can occur at an appropriate time, such as when an issue of concern arises.

"In my opinion, Defence must acknowledge the ubiquity of social media in the communications age, learn to harness its power for recruiting and welfare purposes, and formulate robust guidance to soldiers and commanders in order to balance the need to safeguard our operational and communications security whilst exploiting the opportunities social media presents. The Cold War is over. This is the age-old battle between our Intelligence and Public Relations Corps. Our intelligence and security services disseminate information based on the need-to-know principle. This is often victim to mission-creep, resulting in the release of no information and is at odds with the culture of our public affairs branch, which preaches the benefits of openness and transparency. We have forgotten that we are engaged in a permanent hearts-and-minds operation with Australian society - one that we are currently losing. Defence has already lost too much credibility in the public eye due to its inability to keep up with the 24/7 news cycle. It needs to entrust its people with the power of their own voices, views and opinions. Only through improved awareness of our institution, culture and values can the Australian public truly believe that we are an organisation worthy of their loyalty, respect and admiration."

(Anonymous response by Defence personnel)

3.2 MORALE

Morale is defined by Weakliem and Frenkel (2006:337) as ‘a general orientation that may influence intentions and ultimately behaviour’. Managers of organisations in a study by Bewley (1999:48) believed almost universally ‘that morale had an important effect on productivity’.

Military organisations have an obligation to the general public to ensure the wellbeing and morale of service personnel, in order to maintain a strong force and the security and safety of the community. The high morale of service people and its effects on productivity and general wellbeing are keys to the success of any military organisation, and social media use can affect morale positively or negatively.

3.2.1 International best practice

Communication with family and friends

Isolation and stress among service people while on deployment and away from family and friends for long periods are significant issues for any military organisation. Stress can result in the externalisation of frustration and anger through misbehaviour in the workplace (Rotter and Boveja 1999), and cases of extreme stress can even lead to suicide (Levin 2010).

Suicide is increasingly prevalent within the US armed forces, and a US DOD taskforce has recently released a report calling for the creation of a suicide prevention division (US DOD 2010:ES-9). Steps to reduce feelings of isolation and stress among service personnel by improving morale have been a focus for attention for the US DOD over the years.

Work by researchers such as Rotter and Boveja (1999) shows how intervention strategies can be developed to ease stress among deployed personnel. Research shows that facilitating communication with family and friends is an effective method (Lanigan 2008).

In the past, families and friends of deployed soldiers often had to wait patiently for a letter, and time zones and sometimes poor phone connections meant that contact could be limited or strained. However, recent advances in technology have resulted in personnel being able to access their Defence email, and a suite of social media tools is now available to help them to communicate in real time through messaging, video or audio chat, and status updates.

Early on, it was recognised that electronic media alter the significance of time and space for social interaction generally (Meyrowitz 1985). Some suggest that social media have made people more antisocial, causing them to only communicate online (Wong 2009). On the other hand, bans on social media use, such as were applied by the US Marine Corps in late 2009 (USMC 2009), were criticised for ‘demoralising troops’ and for potentially hindering ‘the development of an information sharing culture in the military’ (Bronk 2009).

The international consensus is that effective communications between service people and their loved ones benefit the service person, their family, their friends, the organisation and the community as a whole. Good morale among service personnel (and their families and friends) fostered through the use of effective communications, including social media, also leads to the organisation being perceived in a positive light and staff becoming potential advocates for the organisation in the social space.

Communication from the military

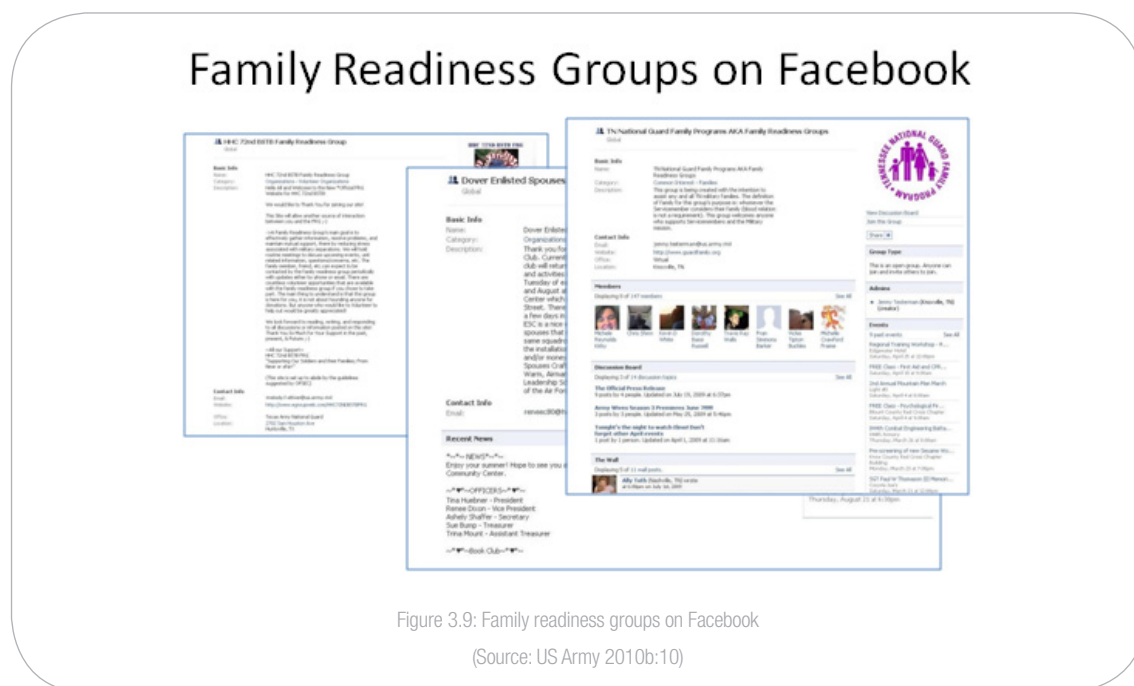
Creating and maintaining a positive brand endorsement among the family and friends of members can also be a responsibility of the military organisation. For example, the US Army employs its social media resources to promote a ‘soldiers and families’ day, which is dedicated to family-based communication using Facebook pages (Figure 3.8). The US armed forces also use their own social media presence to communicate with families and friends, and supports ‘family readiness groups’ (FRGs) to update people on what is happening within the organisation (Figure 3.9).

U.S. Army Social Media Strategy for the week of: <u>Week</u>					
	Monday	Tuesday	Wednesday	Thursday	Friday
Theme:	Question	Facebook feature	Sharing stories online	Women's Equality Day	Soldiers and Families
LOE:	Strategic Environment	Equip and Train	Equip and Train	Strategic Environment	Soldiers & Families
Click:	Pull 3-5 photos from various sites	Pull 3-5 photos from various sites	Pull 3-5 photos from various sites	Pull 3-5 photos highlighting women in the Army	Pull 3-5 photos highlighting Military Families
Photo of day:	"Convoy Fights off Insurgent Ambush" 6,075 total views	"The Wall Hanger" 7,373 total views	"In the Early Morning Light" 3,888 total views	"Don't Look Down" 6,086 total views	Soldier/Family Oriented
Facebook:					
#1:	#1: Photo of the Day	#1: Photo of the Day	#1: Photo of the Day	#1: Photo of the Day	#1: Photo of the Day
#2:	#2: Question: "Army Inspiration" (over 1,330 comments)	#2: Highlight "Ft. Benning" on iTunes	#2: G/8 Video (Army Modernization)	#2: Women in Army History (army.mil/women)	#2: Family Tour BCT (army.mil feature)
#3:	#3: Birthplace of National Guard (army.mil)	#3: Promote Army Videos on iTunes	#3: Promote Women's Equality Day	#3: Personality Profile of Women Soldier	#3: Question: Improvements in supporting Military Family
Tweets:					
#1:	#1: Photo of the Day	#1: Photo of the Day	#1: Photo of the Day	#1: Photo of the Day	#1: Photo of the Day
#2:	#2: Trivia: 7 Core Values (over 10 responses)	#2: Cross-promote "Ft. Benning" on iTunes	#2: Cross-promote Army Modernization Video	#2: Trivia: 1st Women Generals?	#2: Cross-promote Army.mil feature story
#3:	#3: Question: "Army Inspiration" (over 25 responses)	#3: Promote Army Videos on iTunes	#3: Promote Women's Equality Day	#3: Shout-out to Female Soldiers (about 20 responses)	#3: Question: Improvements in supporting Military Family
Blog:	"To Protect & Defend"-Army Inspiration	Army Blog Feature (Army Technology)	Bloggers Roundtable (Unmanned Aircraft Systems)	Personality Profile of Sgt. Tyisha Dorsey (over 1650 FB shares)	Photo Slideshow of "Welcome Home" Celebrations
STAND-TO!	Pain Management	Soldier Athlete Initiative	Comprehensive Soldier Fitness	Women's Equality Day	Army's Land War Net
Goal:	To educate & engage with audience	To promote external Army initiatives & to inform audience	To inform Soldiers & audience of advances in Army technology	To inform/educate audience on Women in Army History	To engage Military families
Measure of Effectiveness	FB: 3 posts; 629 likes, 120 comments (aver. per post) Twitter: 4 tweets; 42 re-tweets Blog: 3148 page views	FB: 3 posts; 615 likes, 138 comments (aver. per post) Twitter: 3 tweets; 47 re-tweets Blog: 3190 page views	FB: 3 posts; 1105 likes, 163 comments (aver. per post) Twitter: 3 tweets; 50 re-tweets Blog: 3,563 page views	FB: 3 posts; 1133 likes, 131 comments (aver. per post) Twitter: 4 posts; 51 re-tweets Blog: 3,010 page views	FB: 3 posts; 850 likes, 175 comments (aver. per post) Twitter: 3 tweets; 56 re-tweets Blog: 4,392 page views

Figure 3.8: Five-day social media strategy template

(Source: US Army 2010a)

Having a ‘soldiers and families theme for a day’ of social media can engage all parties, recognises families as important and that their questions and feedback are highly valued by the US Army. As the themed days on social media might not occur frequently it is important to have other lines of communication to families. *Family Readiness Groups* or FRGs are utilised by the US DOD as a channel through which to pass on information to families. Examples of US Family Readiness Group examples are depicted in Figure 3.9.



Families also use the FRGs to communicate with the US DOD, which ensures that communications going to the defence force come from fewer separate sources. FRGs use social media (among other forms of communication) to create online communities in which families have discussions and provide a support network for each other during times of need. Two consequences are better morale and a positive feeling about the service personnel and their organisation. In turn, this has positive effects on perceptions of the organisation’s brand: service people, their family and friends can act as ‘brand ambassadors’.

Communication misuse

Misuses of social media communication largely involve the sharing of too much information, or sensitive information, with family or friends. The problem was demonstrated in the US Marine Corps’ Basetrack project in March 2011, which was designed to provide more information to those outside Afghanistan by using videos, audio interviews, articles and mapping tools. Family members posted information on operations in Afghanistan on a Facebook page, but the corps felt that the information was too sensitive to be in a social space (Ackerman 2011).

Armed forces obviously have a public obligation to ensure that OPSEC is maintained and that sensitive material is not shared from service people to family and friends. The US DOD responds to online privacy concerns using a proactive approach. Education on what can and cannot be shared online is used as a preventative measure (see ‘OPSEC for families’ and ‘OPSEC for defence personnel’ in Section 3.1.1). This review found no documents supporting the use of punitive responses to social media misuse by US personnel. Instead, the US DOD simply requests that the person remove offending posts from social media. It has not documented any case in which further action was required (US Army 2011:33).

3.2.2 Defence practices and attitudes

The morale of Defence personnel is influenced by a wide variety of interest groups outside the organisation, such as the media, politicians, family, friends, military commentators, Defence alumni and veterans.

Public relations and marketing play a key role in promoting the actions of Defence to the general public, but word of mouth and social media also play a part in maintaining morale. Through the use of social media, Defence has been able to engage some of the smaller interest groups in discussions with the organisation and with one another.

Moreover, many Defence members see social media as a way to deal, at least in part, with the challenges of distance and separation from family and friends.

Partners and dependants

The wellbeing of Defence personnel and their partners and dependants has received much attention. Defence dedicates significant resources to supporting families through the Defence Community Organisation, which provides guidance on how to adjust when a family member is posted interstate or overseas, family counselling and a wide range of other services. The Defence Community Organisation also publishes *Defence Family Matters*, which is a free tri-annual magazine for Defence employees and their families that addresses matters relating to family and provides information on available resources. In addition, Defence Families of Australia is a ministerially appointed group made up of Defence partners. Such mechanisms use Defence resources to help personnel find a work–life balance and to support their personal wellbeing, resulting in a more positive Defence culture, better morale, greater commitment by members, and better workforce retention.

“With the operational tempo being as high as it is in the department of defence, it is imperative that the ADF remains cognisant of the fact that it is the families that are left behind. PUSH Publications, such as Defence Family Matters Magazine should look at educating/reminding families about personal security issues as to see them not openly advertising that they are not home alone etc.”

(Anonymous response by Defence member)

Family members of Defence personnel may benefit from some guidance about what should and should not be said in the social media space, about how much information they can expect to receive from their loved ones, and about how to protect their privacy and security.

Official social media for families

Defence families show great respect for the duties of serving members, the Services and Defence as a whole. Many follow broader Defence activities through social media because it enhances their connection not only with their loved ones, but also with the wider Defence community.

Although many family members rely on the official pages of the Navy, Army and Air Force, they often want to find out more about a loved one who is in a specific unit, especially when that person is in theatre. Anecdotally, these families appreciate the information that official social media channels can deliver, as it gives them a sense of being connected, despite being far away and having limited communication through other channels. One good example of official social media use to achieve this was the Navy's 11:54 minute YouTube video of Christmas messages from HMAS *Melbourne*. The video was highly regarded and received a positive feedback from the family members of deployed personnel.

Multimedia content, images and the down-to-earth tone of social media reinforce a sense of community engagement in an authentic, human way, greatly benefiting morale. However, the benefits are hard to quantify. Defence cannot rely on the volume of fans/followers in social media to gauge effects on morale, as some pages are targeted at niche audiences that are highly engaged anyway. By establishing a baseline for overall sentiment and assessing the frequency of page visits, Defence could gain a much more powerful insight into the strength of particular social media pages. Some groups within Defence already engage with families offline to find out what they expect or want from social media communications. The feedback indicates that many families are highly engaged and frequent users of official social media, with a very real expectation that Defence will continue to facilitate that engagement.

Figure 3.10 shows some examples of interactions on official Defence pages.

 **Royal Australian Air Force** added 2 new photos to the album **Joint Airfield Activation**.



Joint Airfield Activation
Mission Impossible? The Air Force's 381 Expeditionary Combat Support Squadron have convoyed into a Forward Mounting Base three hours out of Rockhampton, Queensland, to stand up a fully functioning air base within 36 hours. Yes, 36 hours to activate an airbase from scratch! 381 ECSS are going to keep us posted on their adventures as they test their skills during a Joint Airbase Activation exercise! Keep an eye on our page for posts, photos and videos.

 Monday at 6:02am · [Share](#)

 126 people like this.

 Amazing exercise! Go 381!!
July 23 at 10:43am ·  1 person

 **Royal Australian Air Force** Day 7 – Check us out! 381 Expeditionary Support Squadron are coming to the end of the first week of the Joint Airfield Activation and we thought you might like to see some of the faces of the exercise! Check out the pictures, and get to know the guys and girls of 381ECSS.
Sunday at 9:42am

 LOOKS LIKE U R ALL DOING WELL GOOD ON U ALL WELL DONE.
Sunday at 10:26am ·  1 person

 Thanks for the photos. My son is in 381ECSS and he's up there at the moment, so I can follow his journey through the daily uploads.
July 20 at 9:04pm ·  4 people

 Thank you for lovely photos
July 21 at 5:15am ·  2 people

 **Royal Australian Navy** added 11 new photos to the album **Recruit School – GE295 – Getting Division**.



Recruit School – GE295 – Getting Division
Week 4 Recruit Comment: This week was our most physically and mentally challengi...
[See More](#)

 July 22 at 1:04pm · [Share](#)

  and 54 others like this.

 I think i can see my  in some of these photo's :D makes me happy to see what they are up to at the moment
July 7 at 2:16pm

 yay for more piks iv seen  in a few of these so happy about it
July 10 at 5:33pm

 Ge259
July 15 at 11:00am

 Ge259  represent
July 15 at 11:01am ·  1 person

 Great photos and wonderful to see loved ones
July 15 at 4:29pm

 Finally some photos of  yah !
July 16 at 1:39pm ·  1 person

 295?? GEEES, I feel old now!
July 22 at 1:09pm

 I bet they are glad that weeks over,
July 23 at 3:59pm



Figure 3.10: Interactions on official Defence pages

"Policing of posts should occur to ensure no derogatory posts. Regiments and Brigades should have their own pages and should convey the good work that occurs along with social information such as sporting and community events the unit is involved with IOT encourage more of a family link to the unit, e.g. families of deployed members from the unit should be able to be invited to family days etc. on the Facebook page."

(Anonymous response by Defence member)

Continued and relevant education and training for all rank levels. The training needs to be current and must be orientated around what social media applications are available at the time. Additional training and education should be made available for the immediate family of serving members.

(Anonymous response by Defence member)

Unofficial social media for families

Many of the Defence-oriented community groups that share information through *Defence Family Matters* are beginning to establish a presence on Facebook and other social media sites. They use the sites as a convenient and cost-effective way to communicate and to reach out to families posted throughout Australia and overseas. Some groups are highly targeted and only have a few members, but the benefit of the pages cannot be evaluated solely by counting numbers of fans or likers. Some of these groups are actively engaged on a daily or weekly basis. Examples include:

- Defence Families Maitland
https://www.facebook.com/home.php?sk=group_179557818727594
- Woodside Defence Families Association
<https://www.facebook.com/pages/Woodside-Defence-Families-Association/150931658267925>
- yourdefence.com.au
<https://www.facebook.com/YourDefence.com.au>
- Cairns Defence Community and Recreation Centre
<https://www.facebook.com/DCRC.Cairns?ref=pb>

Social media provides a valuable resource for people to interact, particularly over vast distances. Properly managed by the people using the media, the system generates few risks. Unfortunately few people have the risks explained to them, (no real social media training) and high-risk behaviours are prevalent. At this time only a minimal amount of these behaviours cause damage, but this could grow exponentially.

(Anonymous response by Defence member)

Veterans, enthusiasts and historians

Social media have enabled many veterans to celebrate their contributions to Defence and maintain a connection to the organisation (Figure 3.11). Many children and grandchildren of veterans have recognised the contribution of their loved ones by commemorating their work through social media channels.



Figure 3.11: Veterans reminisce online

There is a notable amount of online activity celebrating historical milestones in Australia's Defence history, such as 'This day in history' posts and photos of historic ships and planes. Many people also enjoy viewing videos and photos of Defence people and equipment and of recent exercises, such as *Exercise Talisman Sabre 2011*.

Within this space, content is truly a major driver of engagement. This community engages with Defence and appreciates the time and effort contributed by the organisation's social media teams. Defence is doing a good job in providing a balanced mix of content in this area.

General community consciousness

Defence has demonstrated that social media can be highly effective channels to deliver its messages with honesty and integrity and to enable Defence and the Services to tell their own stories. Although much of this engagement has a marketing and public relations purpose, a significant proportion is purely community outreach. Defence social media teams have delivered some rich and engaging content with the limited resources available to them (Figure 3.12). This ongoing communication with the general public and the Defence community about aspects of Defence life is likely to produce more positive opinion and therefore has a beneficial effect on overall Defence morale.



Figure 3.12: Community members discuss the ADF online

Negative comments and risk minimisation

Negative posts will always occur in open social media spaces, but Defence can minimise damage by managing its channels appropriately. The social media teams demonstrate an ability to respond and pull down posts quickly, and their work is viewed positively by most channel users. Many individuals who are following Defence are extremely understanding and protective of the Services. They have also shown their own willingness to monitor the content and comment about those who post inappropriate material. Figure 3.13 demonstrates the overwhelmingly positive reaction from followers when inappropriate posts on the Army's Facebook page were removed.





Figure 3.13: Users support competent page administration

“There will always be good and bad aspects of all new technologies, especially when they involve rapid exchange of ideas, consolidation/networking of like-minded groups, especially when some of these groups are inherently at odds with each other. However, there is a LOT of good that can come out of such network (Egypt uprising etc.) which allows coordination and social change. It’s exciting to watch, and exciting to be a part of it. There may be negatives, such as bullying, but this happens in the real world face to face as well - but I don’t think anyone would suggest complete segregation of individuals so as not to have any negative consequences lol.”

(Anonymous public comment)

“I am concerned that Facebook could be used to compromise my position in Defence although I would not allow myself to fall into that position, however I do not want to lose the medium that allows me to keep connected with family and friends.”

(Anonymous response by Defence member)

3.2.3 Discussion

Social media can be useful in reducing the effects of isolation and stress, which are two key contributors to low morale, although Defence Restricted Network and ICT limitations and internet access provide ongoing challenges. Open lines of communication between troops and their loved ones help to ease the stress of deployment, and have positive effects on families and friends by easing their own stress about safety concerns.

The Services' primary pages have already begun to gain significant traction, and now Defence might consider the need to provide additional resources to support the social media pages set up for particular units and their families. Nonetheless, Defence will need to continue to assess new ways of facilitating electronic communication. These pages are particularly valuable to the men, women and children at home and regardless of whether there is access to social media by Defence personnel in theatre, content can be provided via other means to the social media teams for ongoing management and uploading.

Defence's social media presences have overlapping audiences with a desire for more information, genuine conversation and a place to gather online, and the organisation could be said to be fulfilling that desire. There will always be a need to support troops and their immediate families, but a balance must also be struck to address the desires of veterans, enthusiasts, potential recruits and the general public. By increasing the forward planning of content throughout the year, clearly articulating policies and enabling personnel with the appropriate tools to contribute, the opportunities for Defence can be maximised.

Defence should grasp opportunities to provide unofficial page administrators and families with some additional direction on what content is safe to post. By providing families with tools and guidelines through the Defence Community Organisation, Defence Families of Australia and Defence Family Matters magazine, the organisation can effectively minimise risks associated with this aspect of social media.

3.3 MARKETING

For any organisation, marketing is an important tool for promoting its goods or services and enhancing its reputation in the marketplace. Defence uses marketing strategies to recruit members, maintain its reputation, enhance morale and retain personnel.

This section summarises and provides examples of best practice in the military use of social media for marketing, which includes branding, public relations (PR), communications strategy and content publishing.

3.3.1 International best practice

The international consensus is that social media can be a potent device to market defence organisations.

Branding

Social media are used extensively by international military organisations to reinforce their overall brand images and those of their individual services, commands and members. This section provides examples of how military organisations have successfully leveraged their brands using social media, with a focus on top-level, longer term brand strategy, as opposed to individual marketing campaigns or promotional activities.

A brand is not just a logo or an emblem. It's an organization's identity.

The Army's brand is one of strength. Everyone is familiar with the Army: the Apaches, the Humvees, the weaponry and the push-ups. But the brand brings everything together in a clear and recognizable visual presentation.

When people see the Army's brand, they know what they're going to get, and that's important when maintaining effective and informative social media presences

(US Army 2011a:3)

The US Army and US Navy stand out as examples of strong brand images in social media, with the same standard of representation across most forms of media. Other countries have been more cautious with their launches into social media, although there are also examples of effective use in the United Kingdom, Canada and New Zealand.

The US Army uses its social media strategy to create conversation, ask questions, create dialogue, and generally get people talking (Kyzer 2011). That engagement is then used to improve services and to generally improve relations between the Army and the community. However, the US Army is cautious about protecting its brand and about general marketing activities that might conflict with its values and goals. That caution is demonstrated by its special agreement with Facebook, which has resulted in the US Army Facebook page not containing any advertising (US Army 2010a).

Every American ‘soldier’ (or Army employee) is responsible for upholding the brand values of the defence forces by, for example, how they wear their uniform, their attitude towards their employer, and, more recently, how they publish content on social media. Section 3.1 of this report notes that the US Army’s social media practices are governed by existing policy covering other forms of media, and that the online behaviour of its personnel is expected to be as exemplary as their offline behaviour. Through educating military personnel about how to interpret regular policy in a social media context, the US Army has successfully translated its positive offline brand image to social media.

The US Army best practices handbook states frankly, ‘If you’re not willing to lose control of the message, and give some of the power to your community, social media is not for you’ (US Army 2010d:2). This message is used to warn commanders of the brand risks associated with establishing a presence in social media, despite the Army’s bold movement into social media without clear policy.

Guidelines for branding in social media

In an attempt to combat potential loss of brand control, the US Army provides guidelines to commands for establishing an ‘external official presence’ (EOP) (Chang 2010), which is any officially approved and managed presence on a social media site or service. Rather than stipulating specific rules, the memorandum provides guidelines on how to make decisions that protect and enhance the brand when using social media.

A 25-week series of social media seminars run for US Army employees paid significant attention to marketing-related subjects, and included an entire seminar dedicated to the branding of social media presences (US Army 2011a). The presentation material offers the following key points for Army personnel in charge of social media or EOPs:

- Use approved artwork
- Use the right resources
- Select the right look
- Unify the look on all platforms
- Mix it up for special events.

The US Army has also established the US Army Brand Portal website (US Army 2011c), which houses brand elements such as approved logos, camouflage backgrounds, colour palettes, typography and photography. Managers of EOPs can download the resources they need, which ensures that they stay consistent with the overall Army brand while still having the freedom to represent the unique aspects of their commands through the content. Figure 3.14 shows a screenshot of an online branding guideline.



Figure 3.14: US Army online branding guideline

(Source: US Army 2011a:4)

The US Navy also provides information to employees about how to use and leverage branding in social media. *Managing audience engagement to gain and retain public involvement* (McInay 2010) describes how personnel can involve the public with the Navy through social media while at the same time upholding the brand values of the organisation (Figure 3.15). The US Navy is clearly aware of the value that social media can add, and so has committed significant resources to include social media in its overall communication plan (McInay 2010).

- Transparent
- Conversational and professional
- Answers questions and avoids arguments
- Listen to our audience

(Reference US Navy Managing Audience Engagement to gain and retain public involvement)

Figure 3.15: Top-level brand values underpin the US Navy's educational material for social media engagement

(Source: McInay 2010)

Official and unofficial presences

Anyone can potentially create an online account that pretends to represent a military service. This action may be motivated by malice, but sometimes a member of the public inadvertently creates risks for the forces through misplaced good intentions.

To reduce the proliferation of unofficial military-related social media accounts, the US Army publishes a list of official social media presences in all of its official digital marketing material and in many printed brochures. The list is also available for printing in a business card size, and it can be pressed out of presentation materials as a pocket reference card (US Army 2011d).

Furthermore, it is US Army policy (US Army 2010b) that all official social media accounts must be submitted to the official Army website for inclusion in the directory. This is not only helpful for the branding of individual unit command pages, but also provides certainty for stakeholders and members of the general public who might otherwise become victims of hoaxes or scams. These situations can easily happen, as official Army presences can be difficult to find among the unofficial ones. For example, it is unclear how Facebook results are ranked in searches for specific keywords, and the official US Army page is not listed in the results of a search for 'US Army'. Official presences (Figure 3.16) must be heavily promoted, as they are not discoverable using the expected search terms.



Figure 3.16: Official social media presences of the US Army

Branding is not just a visual exercise, but a security measure that helps to protect the general public from fake pages created with malicious intent. If unofficial presences are damaging, they may be reported to the social network owner. The use of a logo without permission infringes copyright law, and a request can be made to have a page closed down for unauthorised use of protected graphics.

Capitalising on events

The US armed forces have social media content strategies at both the organisational brand level and the individual command level. For example, the US Navy Special Warfare Recruiting team successfully used social media content covering the departure

of a ship to leverage traditional media coverage and generate positive community opinion. In 2010, the team aboard the USS Abraham Lincoln made their deployment date a marketable event, using social media to tell the story of their departure (US Navy 2010a). Most notably, the Commander of Carrier Strike Group 9 started a vlog (video blog), and video updates about personnel, equipment and the mission were also posted to Facebook. This gave people in the wider community an opportunity to connect visually and emotionally with the personnel on the ship. A highly rating US breakfast television program, The Today Show, used this content to tell its viewers that the ship was about to be deployed. Continual postings throughout the deployment kept the community engaged, allowed it to feel involved in the mission from a distance, and also included a recruitment message. The video content provided a rare look into life aboard a US Navy ship, allowing potential recruits to see what they might experience if they joined the Navy.

In this example, the Navy achieved multiple results – reaching stakeholders, traditional media coverage, additional social media coverage and deeper public engagement with the brand. This was all achieved at minimal production cost and without additional investment in advertising or PR.

In such cases, content can be generated both by the organisation and by individual participants. Individuals may generate and share supporting content, especially if the event is about them or their friends, family, interests or personal values. Some may post several times over a long period about an event that interests them and their network. Overall, content can include the event announcement; details, photos or videos of the venue; details such as medal recipients; live updates on the event; post-event photos and videos; and event feedback.

Leveraging public events

Veterans Affairs Canada's 2009 remembrance celebrations were an example of the successful use of social media based on a planned event. Veterans Affairs published remembrance messages on Facebook (attracting more than 175,000 fans) and posted a Veterans' Week vignette on YouTube (viewed by 32,000 individuals).

(Blackburn 2010)

Generating and publishing content

It may not always be obvious to a social media user how content posted into social media can breach security, damage brands, or simply not support the values so carefully marketed by an organisation's communications team. Therefore, many military organisations have devised guidelines for social media use that help to protect their brand and security.

The US Army content checklist (Figure 3.17) is a quick reference guide for managers of EOPs when publishing content to Facebook. It is designed to make military publishers stop to consider key points before committing content to the social media space. The key points range from marketing strategy to OPSEC considerations, ensuring that content is suitable, effective and safe.

Facebook quick reference sheet – techniques learned from the very best pages

Do:

- Start with a strategy – how does social media fit into your overall communication goals?
- Scatter your posts throughout the day; do not clump all together
- Post on weekends and evenings, and evaluate which time works best
- Tag at least one other page in each post
- Try to ask an engagement question for every post
- Respond to questions in a timely manner
- Post and follow a comment policy, and enforce it
- Remember to post in a friendlier tone, but not unprofessional
- Spell check every post prior to posting
- Thank your followers and praise them often
- Use lots of quality photos (be sure to add as many details about the photo as possible – or ask your audience to add details as an engagement item; also ask them to tag themselves or others)
- Use short, raw, catchy video
- Ask yourself: would I share that with my friends?
- Mix it up: photos, questions, videos, sharing others' content, news stories, etc.
- Add a personal touch; connect with your audience
- Set defaults to show only your posts first (after all, this is a command information platform, and this allows your message to be seen first, and allows others to still comment on your wall)
- Welcome participation, collaboration, and feedback
- Get a short, smart vanity URL (facebook.com/username) (available only after 25 followers)
- Update top 5 photos often (show a variety of activities, angles, personnel, etc)
- Have someone else read your posts before you post them (to see if they make sense)
- Track metrics and evaluate how content performs. Determine what metrics are important to you before you engage, set a benchmark and track over time.
- 'Like' sister or similar organisations, and tag them often
- Post information or comments on other pages, while using your organisation's page (be mindful if you are posting as organisation or business)
- Always use OPSEC when posting
- Identify/find SMEs to answer questions that come up on your page, or direct them to SME
- Avoid using automated posting services to post same content to multiple sites
- Ask your followers what they would like to see on the page

Don't:

- Post too many times a day (you will lose followers)
- Clutter all your posts at one time
- Do not be too promotional
- Use boilerplate messages or snoozy press releases, unless necessary
- Use social media (teen) language in professional posts (ex: I wanna b ur bff 2day & 4evr)
- Use geo-tagged programs on your page (ex: showing where you are Tweeting or FBing from)
- Post a link without giving some sort of lead, description, or call to action
- Remove content just because you don't like it. If it doesn't violate your comment policy, leave it!

Remember:

- You do not control what happens to a message once it is posted
- It only takes one unprofessional slip to taint a reputation
- If you do not have a lot of time to monitor, then set tighter restrictions (photos, videos, comments, etc.)

Figure 3.17: US Army Facebook quick reference sheet
(Source: US Army 2010a)

The British Ministry of Defence takes a more direct approach, telling users what is and is not acceptable. Its guidelines assist military personnel who have the best intentions and a solid understanding of OPSEC, but who may not be aware of the risks associated with posting some content. For example, the British Ministry of Defence offers more specific guidance on the posting of images than that generally provided by the US DOD (Figure 3.18). It states that 'pictures are powerful and often revealing assets, and while photos can contain trivial information they can also pose a risk to personal and operation security if placed in the wrong hands' (BMD 2011).




In general, you should avoid:

- Operational security breaches; images that disclose location, operational intentions, equipment specifications and capabilities
- Images that could damage your Service's reputation
- Aggressive, abusive or inappropriate poses in uniform
- Identifying yourself or other personnel on operations
- Videos that display specific locations or operational intentions

Figure 3.18: British Ministry of Defence guidelines for the use of images in social media

(Source: BMD 2011)



The big picture/content strategy

Social media content must always be considered in the context of the organisation's overall branding and marketing strategy. In other words, the use of social media by localised groups or individuals should complement, not conflict with, overall content strategy. For a specific event, the content should reflect the overall promotional strategy with a clear goal to promote the event. However, the overall strategy for content beyond social media has to be considered to ensure that content does not conflict with the organisation's or command's vision and goals.

Significant stakeholder engagement is needed to develop a content plan. To manage that task, the US Army has a detailed a fiveday social media content template (*Figure 3.8 in Section 3.2.1*), which is integrated with its overall communications strategy. The template covers themes for each day: Monday is question day; Tuesday is feature day; Wednesday is for sharing stories; Thursday is dedicated to women's equality issues; and Friday is soldiers' and families' day. Guidelines are also provided for each channel, including Facebook, Flickr, Twitter and blogs. The content strategy clarifies the goal of the content and measures its effectiveness through documenting photo views, 'likes' and other statistics.

The British Ministry of Defence has also acknowledged the need for new strategies and processes in the development of content to mitigate potential conflicts across media. The Defence Editorial Board has been established to plan content, as a step towards a united content strategy that considers the often complicated and conflicting needs of multiple stakeholders (M Crane, pers. Comm., 6 June 2011). The group meets three times a week to discuss current objectives and how they will be communicated throughout the different media channels.

Public and employer obligations

Military organisations use social media to help meet their public and employer expectations, to champion certain causes and to provide information of interest to the community about the organisation's role in society. The US Army's fiveday content template helps the Army meet both its public and its military obligations. For example, Thursday is dedicated to the subject of women in the army, which supports the employer obligation and reasonable public expectations about equity. This results in multiple outcomes: first, it generates social media engagement with women and the general community; second, it drives traffic back to the main website (*Figure 3.19*), where the content is archived to meet public record-keeping obligations.

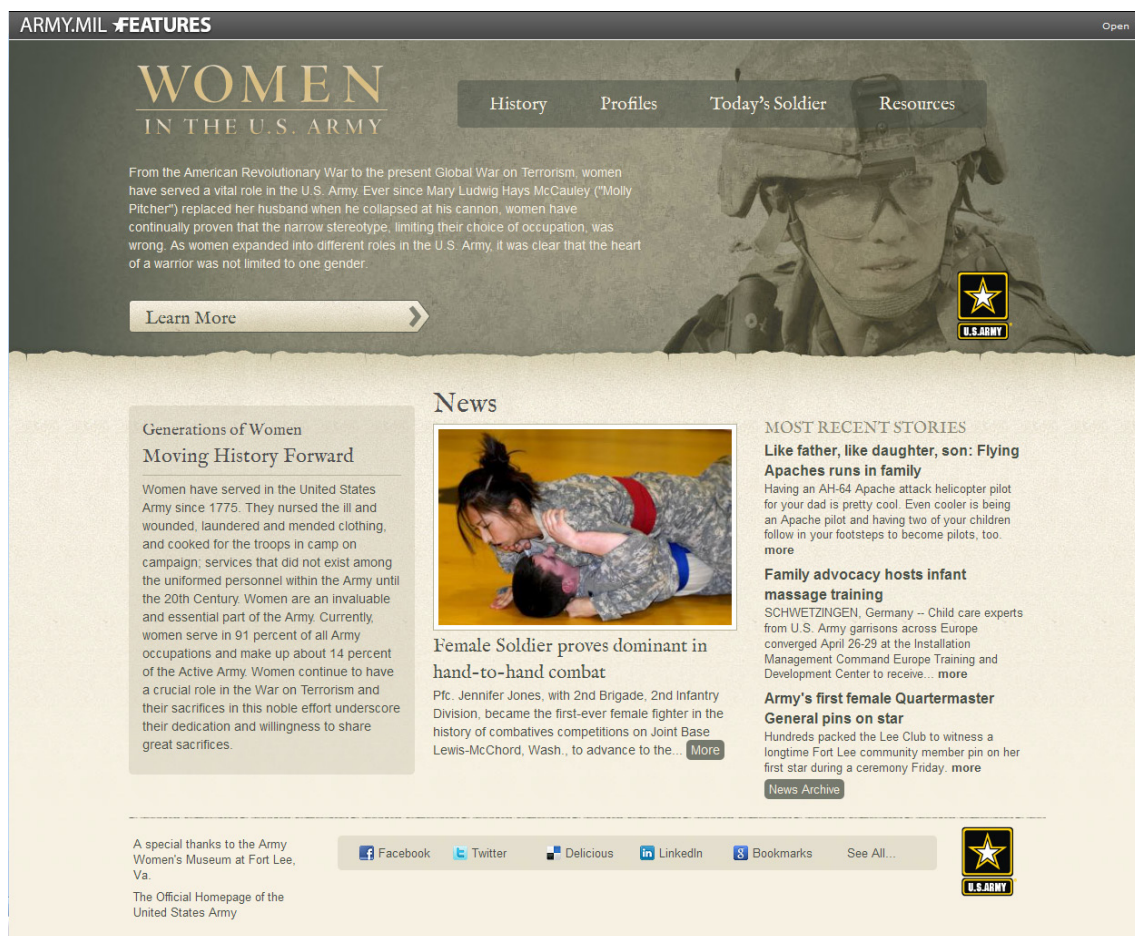


Figure 3.19: Women in the US Army web page
(Source: US Army 2011e)

The five-day content plan template is also a measuring tool. It is filled in each week with details about what activity has occurred and how many views, likes and comments each piece of content received. Measuring the success of different themes is also possible by comparing views, shares, and likes on a per topic basis. This structure gives stakeholders an opportunity to assess content success and identify areas that could benefit from positive social media engagement. The template enables a formulated effort to increase engagement with the community, families and target audiences for marketing campaigns such as recruitment initiatives or celebrations such as Veterans Day.

Integrated public relations

In the United States, in particular, military personnel are given responsibility for being 'marketers' and are encouraged to engage in social media. However, this can create some challenges from a PR perspective. Individuals might not have the required training to communicate effectively on behalf of the organisation, and therefore require guidelines and advice to achieve positive marketing for Defence brands. Many military organisations use training programs and guide documents to meet that need.

The US Air Force focuses on how social media can extend traditional communications and PR activities. Guides provided to Air Force personnel explain basic tactics that complement traditional forms of internal communication, community relations and media relations (US Air Force 2009). A focus on entry-level education provides a clear path for Air Force personnel to understand what is and is not expected of them in social media use, reducing the risk of inappropriate activity and ensuring that traditional media activity is supported and complemented.

Social media and the internet in general store and organise extensive information, which makes them popular destinations for people who want to research topics they have heard mentioned in mainstream media. The US Army uses its official website to house all content, which meets the public obligation of record keeping, but treats social media as a way of releasing information, as opposed to storing it. In the same way that a press release is sent to a traditional media outlet, a link to it can be posted using social media.

An additional benefit of using social media in this way is that the content (the link to the press release) is portable and becomes a simple way for others to share the content with their own networks, thereby increasing the reach of the information. Organisations can also gather information about visitors to their social media sites, which can inform PR strategy.

Traditional broadcasting media outlets also use social media (particularly official channels that publish interesting and current content) to gather stories for news articles or television pieces. Therefore, providing positive content that represents the organisation's brand image can encourage positive media representation through the convenient and efficient delivery of the information.

Responding to conversations

PR crosses media platforms when, for example, a press release generates discussion in social media. To help military personnel respond appropriately when discussions occur, the US Air Force provides written guides with strategies that can be used to respond to social media commentary. The strategies complement traditional forms of internal communication, community relations and media relations. For example, a web posting decision tree was developed by US Air Force PR for use when responding to a comment or request in social media (Figure 3.20).

In social media, conversation is content. This means that responding without consideration of what is being said can create an unintended OPSEC breach or a PR problem. The US Air Force's decision tree shows clear paths for the best responses to common social media issues. The tree differentiates between when a conversation should be addressed and when it should not, such as when the poster's intention is to cause trouble (which is the aim of 'trolls').

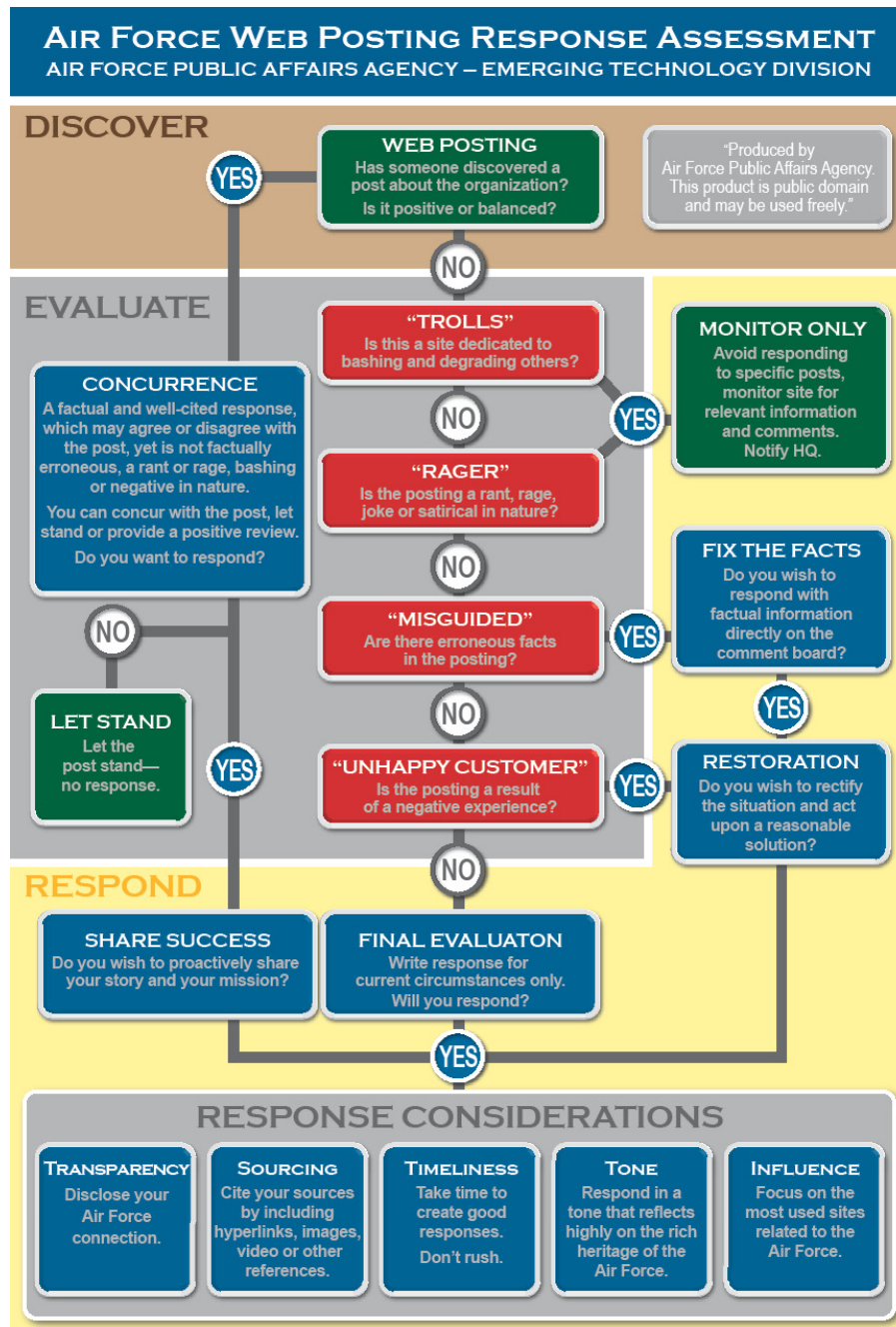


Figure 3.20: US Air Force web response decision tree

(Source: US Air Force 2009)

Community engagement and building trust

The USS *Abraham Lincoln* case showed how community engagement can be achieved by sharing content about marketing or PR activities. When social media are used, control of the message may be lost by the organisation that the conversation is about. However, centralising conversation in a primary location, such as a Facebook page or a blog, means that the organisation is in the conversation and can monitor and respond to it. By keeping the audience engaged with regular releases of relevant content, information can be communicated quickly and cost-effectively. Highquality, regularly refreshed content will draw people back to the site, rather than searching elsewhere.

The benefit of community engagement is the creation of relationships with those members of the public who might act as promoters of the brand. Maintaining positive relationships with the community is an effective way to spread a positive brand message in social media, just as it is in traditional offline PR activities. The difference is that guests and journalists can no longer be identified by their traditional VIP media passes or expensive camera equipment. Everyone is now a potential journalist in the social media world, which is one reasons it is important to build trust and a positive online connection with the community.

The US Navy, which bases its social media policy on the same US DOD documents as the US Army, stresses the importance of honest communications and full disclosure of identity and intentions in order to build long-term trust with stakeholders. Allegations made against the armed forces can create doubt and resentment among stakeholders involved in social media communications. For example, the US Army came into disrepute in March 2011 when alleged leaked emails indicated that the government had hired a PR company to create fraudulent accounts in social media in order to influence conversations (Long 2011).

In the end, effective social media communication is needed to help prevent negative conversation on military social media channels and to build trust in the online community. It depends on those involved feeling comfortable and confident about the ability of the channel to support the organisation's communication goals. The US Federal Trade Commission offers further guidelines for social media engagement (republished by the US Navy) based on two key requirements:

- truthfulness and disclosure from your social media administrators
- monitoring and management of conversations about your command to ensure they are truthful (US Navy 2010b).

The guidelines stress the importance of training personnel about transparency in all communications, including social media.

Measuring results

One of the greatest assets of social media as communication devices is that the breadth of their influence can be measured. The downside is that many social media networks are owned by third parties, which means they own the statistics, which might not be publicly available and might not necessarily be credible.

There is limited available information about international best practice for measuring social media success. The US Army tracks its own results within specific software platforms such as Flickr (Figure 3.21). It advises its social media managers to record all statistics, such as views and shares, so they are able to determine the popularity of specific content. The statistics are published in the fiveday content plan, which allows for analysis and distribution to stakeholders. The result is that the fiveday content template has itself become a measuring tool.

Measuring success

The following metrics will be used to determine success:

- Provide analysis of the number of views of material each week.
- Provide analysis of what photos receive the most views each week.
- Measure the amount of direct engagement with Soldiers, Veterans, Families and the general public by tracking inquiries.
- Record the number of photos we add each week to help determine if higher number of views for the week is linked to more photos being added (and vice versa).
- Track number of photos re-purposed on other sites (i.e. Associated Press, Blogs, etc).

All measurements are crucial in determining how the Social Media Team can better serve its audience. Providing analytics also assist the Social Media Team in displaying the importance of using social media platforms to Senior Leadership.

Figure 3.21: US Army Flickr strategy
(Source: US Army 2010c)

3.3.2 Defence practices and procedures

“The Defence Public Affairs Branch plays a critical role in assisting commanders and managers to promote Defence as a capable, transparent and accountable organisation. In turn, commanders and managers maintain and improve Defence’s reputation by giving the public accurate and timely information, and by facilitating access to Defence personnel and activities ... A failure to engage will mean that public perceptions of Defence are disproportionately shaped by speculation, misinformation or unbalanced reporting. Conversely, by engaging the public through the media, Defence has the opportunity to inform and influence public perceptions.”

(Source: DI(G) ADMIN 08-1, p. 1)

Defence marketing activities primarily revolve around brand management and public affairs, while at the same time supporting recruitment for the Services. The high level of Defence activity in recent years, coupled with the rapid evolution of the media cycle and the use of digital means to communicate, has meant that Defence has had to change how it communicates with journalists and the public. The change has had a significant impact on the organisation, as it has on other government agencies and the private sector.

Defence’s message has remained constant, but its methods and approach for communicating with the broader community have changed greatly. Defence is similar to every other organisation grappling with this issue, which was highlighted during 2008 consultations led by the Department of Broadband, Communications and the Digital Economy.

‘It’s probably worth remembering: as untried as government consultation blogs are at the federal level in Australia, so too are citizens unused to being able to engage with their government in this way. They may be new at it, but so are we—and both sides still have a lot to learn about the other.’

(Source: Snurb 2008)

Although seen by some as detrimental to society, in recent years the social media have also been recognised for the many benefits they can create, from facilitating democratic movements to helping individuals in times of crisis. For example, the Queensland Police Service and the Brisbane City Council used them as significant communications platforms during floods in 2011, after having established social media teams and strategies well in advance of the crisis. Both organisations were able to respond quickly, without comprehensive disaster management response guides for social media. Both were able to learn, adapt and develop their communication processes during the floods. When the brisbane.qld.gov.au website crashed as a result of server overload, the social media team was able to continue broadcasting information reserved for the website and to respond to individual enquiries on the Facebook wall, which ensured that the message could be amplified to a much broader audience. Defence also benefited from social media during the floods, not only in support of the work of reservists, but also in reinforcing their positive humanitarian efforts on domestic soil.

The rapid transformation of communications and news has resulted in many organisations having to play catch-up in their use of social media and their communication strategies more generally. As Martin North, Managing Consulting Director of Fujitsu Australia, commented:

“The fact is this is now mainstream ... there’s a huge challenge there to break out of the mould of the old static content and one-way communication, and into much more collaborative, information-sharing, web-as-a-platform thinking ... my observation is that not many organisations have yet really grasped the full potential of this particular development.”

(Dwyer 2009:585)

The Defence brands

Defence and the individual Services are certainly established brands within Australia. There is much goodwill and pride associated with the brands, not only within the organisations but also among the public. In some cases, however, the poor actions of a few have undermined and reflected poorly on the broader Defence brand.

Defence culture has a focus on planning, preparedness and risk minimisation, which are all critical to any deployment or activity of Defence personnel. However, that focus has also affected the way Defence approaches marketing and public affairs. Many qualitative interviews for this review identified a high level of aversion to the risks in social media engagement, which extends to communications with the media in general.

“While I would never tell a Defence member that they can’t use social networking sites, I believe that there needs to be more consequences to members who post comments and bring disrepute on the Defence force. It is my personal belief that if a member identifies themselves as a member of Defence and then posts inappropriate material, then they should be subject to disciplinary avenues. This is not just to do with OPSEC or official information but also if they were to defame or libel an individual. The reputation of the Defence Force needs to be able to be protected at all times, a small proportion of members bring disrepute to the Defence Force and instantly in the eyes of the media and the general public, it is the culture of the entire Defence Force. I am tired of being branded with the same brush of a very small minority of Defence members ...”

(Anonymous response by Defence member)

Despite Defence's rigorous policies and processes for official communication with the media, there is some resistance among relevant personnel because they are not comfortable about exposing their professional personas or activities publicly. This leads to a somewhat reactive approach to engaging with the media, in which OPSEC is continually cited as a reason for not engaging effectively. As a result, Defence can sometimes devalue its own positive contributions, which could be used to reinforce Australians' pride in the Services.

As one commenter stated, 'Defence relies on "good appearance" to help with recruiting/ public support. If social media content from Defence members is not monitored or the users aren't educated about the consequences then it can cause unwanted media attention.' While this statement is true for content generated by unofficial methods, social media can also be used in an official capacity to:

- deliver a message directly to the public without journalistic interpretation or bias
- communicate directly, in a more genuine and human tone, with the public, interest groups, families and potential recruits
- share information quickly across many platforms to reach a large audience
- enlighten audiences that do not normally follow news in traditional print and broadcast media.

Some of the following quotes were shared in relation to marketing and public affairs for Defence during the review period:

"More education required to ensure OPSEC is maintained. Also education on media and media interaction (such as newspapers, radio, journalists etc). The Defence Force does media poorly. Really, the culture within the Defence Force is that any publicity is bad publicity and must be avoided at all costs - ESPECIALLY if it is an order. Social Media is a great opportunity to build morale and improve recruiting efforts."

(Anonymous response by Defence member)

"Thanks for the opportunity. I think the majority of people in the ADF do the right thing. It is a small minority that step over the line and this causes politicians and some in the general public to go into a feeding frenzy. The fact is that the ADF does tremendous work both at home and abroad. We have very good and committed people. It is not all bad. We deserve some credit from time to time and I am sick of being flogged in the public arena for matters that I have not been associated with. Cheers."

(Anonymous response by Defence member)

A widely held belief about social media within Defence is that it is used by members only for social chatting. In fact Defence has used social media effectively in an official capacity for more specific objectives, such as to:

- tell the story of flood recovery efforts in Queensland
- report on humanitarian support crews deployed to Japan after the earthquake
- promote Anzac Day celebrations
- show historic events in which Defence has been involved
- use high-quality imagery of exercises and operations to support public affairs messages, highlight personnel's professionalism and reinforce Defence's reputation
- humanise the activities of Defence by profiling service men and women in their day-to-day activities
- supply information to people considering careers in Defence
- publicise ships and battalions for those interested in more detailed areas of Defence.

"Defence is in a position to exploit social media; and may indeed use it as a tool to achieve the same objectives as business. However; Defence, as an organisation, needs to temper its activities in the social media sphere in such a way that any messages it places into the public spectrum cannot be hijacked and exploited. As a PA tool, social media promises to be an effective and contemporary enabler that has the potential to reach and indeed target/monitor the desired demographic."

(Anonymous response by Defence member)

Resourcing

Social media teams within the Services are motivated and willing to communicate more broadly. Despite being under-resourced in certain areas, they are achieving engagement that warrants merit, despite some limitations, but they have not had the opportunity to maximise the potential marketing and PR benefits of that work. This is partly due to a lack of timely, relevant and interesting content from units.

One Australian Army campaign that was deemed a success was a recruitment drive for pilots. The team organised a number of Blackhawk pilots to chat on Facebook for several hours. This was supported by other marketing to drive interest in the page on the specific date and time. The Army engaged with more than 800 people on the page and saw a marked increase in enquiries to the 131901 Defence Jobs enquiry line. Some visitors were also retained as followers of the page.

One interviewee reflected that, under current guidelines and regulations, this method of engaging with the public (while highly effective and without complaint or incident) may be deemed inappropriate. This appeared to be due in no small part to the potential for this channel to be defined as 'official' and therefore require prior approval. Clearly, such a requirement would reduce Defence's ability to use social media effectively – which indicates a need to review policy.

Unit advocacy and willingness to engage in social media

Social media are new to a number of commanding officers. In early 2010, DCOORD-A (Office of the Chief of Army) sent an email to Unit Command titled 'Use of social media to support Unit Command' (DCOORDA, pers. comm., 20 April 2010). The email was concise and direct about the benefits of social media, noting benefits for administration and security and opportunities to communicate unit information to soldiers and their families. The high-level recommendations in the email were:

- *"That you **note** that AHQ administers an 'Australian Army' Facebook site that currently has 13500 regular users and is regularly accessed by local and national media.*
- *That you **consider** how your unit may be able to use the media established on Facebook and the Internet to communicate messages and information to your soldiers and families.*
- *That you **note** any media generated by you (stories, video, photographs) can enhance the reputation of Army in the wider public when actively and frequently loaded onto social media such as Facebook and the Army webpage.*
- *That you **note** that there is significant Public Affairs support available in your formation and at AHD to Support your unit PA campaigns should you need further information."*

(Source: DCOORD-A, Office of the Chief of Army, 2010, pers. comm., 20 April 2010)

The email endeavours to be realistic about the use of social media, balancing the needs of those who prefer to follow the Army on its website. It lists individuals who can support units with technology and strategy to produce the right outcomes for each unit. This level of advocacy is extremely impressive, as it demonstrates tangible benefits for commanding officers in using social media for communications.

Defence personnel unintentionally affecting public affairs

The recommendations in this report should help to neutralise the major concerns in Defence about the use of social media. For the most part, the organisation has established professional and relevant official existences in social media channels. Continuing the education of personnel on the broader benefits and risks of sharing Defence information in social and traditional media is a primary concern. Regardless of whether a member shares confidential information online or offline, the ramifications should be consistent and just.

Education about social media needs to be incorporated into training materials, starting from induction. As one member aptly stated:

[T]he use of these forms of communication needs to be drummed into the members of the ADF from the start of their time with Defence due to the ramifications of inappropriate statements being made by inexperienced members that get out and into the public domain and get grabbed by the media and taken either out of context or misquoted and blurring the perception of Defence by the public.

Recruitment


Although recruitment is primarily driven through www.defencejobs.com.au, those responsible for the Services' social media channels report a significant volume of 'soft' enquiries (Figure 3.22). Potential recruits may prefer not to wait in a phone queue, fill out an enquiry form or speak to someone in person.




 **Royal Australian Navy**
what stuff do u need to be in the navy?
July 22 at 4:39pm



 **Royal Australian Navy**  It depends on what job you want to do. The Defence Recruiting website at <http://www.defencejobs.gov.au/navy/> lists the available job opportunities and the educational requirements needed
Cheers
Ray (Navy Admin)
July 22 at 4:44pm

  thanks ray:)
July 22 at 4:45pm

(Source: <http://www.facebook.com/RoyalAustralianNavy>, retrieved 22 July 2011)

 **9 RQR**
How hard is it to transfer from Choc's to Infantry Regs? im tossing up on weather to enlist in 9RQR or 25/49 RQR then transfer to Regs or to go to Reg Artillery then corps transfer to Infantry... what would get me to reg infantry faster? advice anyone? Cheers!
May 23 at 2:51am

 **9 RQR** assumes that you are being told by Recruiting that there are no places in the Infantry . It is very difficult to transfer to the Regular Army from the Reserves at the moment – for the same reason. You may be better off joining fulltime into another Corps and Corps transferring. 9 RQR welcomes advice for  from others.
May 23 at 8:10am

  Thanks for that advice and yes they have told me there a no spots I'n infantry at the moment... So yes corps transfer via regular army looks like the way to go
May 23 at 3:25pm

(Source: http://www.facebook.com/permalink.php?story_fbid=10150198947006561&id=100002331061867, retrieved 23 June 2011)

 **Royal Australian Navy**
hi all, just wondering if anyone knows the restrictions for people with glasses, im really fit but my eyesight isnt great, would that exclude me from clearance diving?
Saturday at 3:18pm

 **Royal Australian Navy** Hi  you should contact a Defence Force recruiter with this type of question.
<http://www.defencejobs.gov.au/recruitmentCentre/contactUs/default.aspx> Cheers Ash (Navy admin)
Saturday at 4:23pm

(Source: <http://www.facebook.com/RoyalAustralianNavy>, retrieved 25 July 2011)

 **AustralianArmy**
hi, i was just wondering how to lodge an appeal to be deemed medically unfit, i was told i was unfit to join but i was not told how to appeal it, thankyou
19 hours ago

 **AustralianArmy** Hi 
My advice to you would be to call 13 19 01 for advice.
Best of luck,
Gabrielle AA Admin
18 hours ago

  ok, thankyou :)
18 hours ago



(Source:http://www.facebook.com/permalink.php?story_fbid=10150245897842639&id=100000630859543, retrieved 25 July 2011)

Figure 3.22: Recruitment enquiries on Facebook

Some individuals rely on social media to seek out the opinions and perhaps the approval of peers. As a result, they often passively monitor pages without posting until they are confident that they will receive an appropriate and timely response. It has been reported that some cadets admit to engaging in social media channels in order to demonstrate their aptitudes and abilities, in an attempt to positively influence the recruitment process. While those allegations appear to be without merit, their existence demonstrates that the public sees social media as a road to recruitment.

The Services' social media presences are inextricably linked to recruitment, so action should be taken to align the efforts of Defence's social media teams and Defence Force Recruiting. That is happening now on a small scale, but has encountered some resistance from individuals who believe that recruitment must be kept as a separate communication stream.

Ownership of 'official' Defence presences

As the review team's audit of Defence's social media pages discovered, some pages are clearly owned and managed by the Services but the owners and managers of others are not identifiable. At the outset of the review, the team requested a list of all social media sites deemed 'official' by Defence, but no list could be provided. During the review a number of people tried to produce such a list, but found that the task required a more concerted and centralised effort than they had realised. Defence appears to have established some of the pages that, which could not be confirmed as 'official', with which use imagery and crests that might infer imply endorsement.

Some of the pages have broken links to the Defence website and are updated only once or twice a month, resulting in low engagement with users (who are perhaps suspicious about the pages' official authenticity). If the pages were created by Defence as official channels, little attention has been paid to their purpose or ongoing management. Regardless of whether they were created by Defence, some of them have a high level of interaction with users, some of whom are current Defence personnel who should be adhering to the *DI(G) ADMIN 08-1*.

The RAAF submitted two policy documents to assist the review team, including Policy for the RAAF internet website and Annex B Guidelines for websites located on the Associations sections of the RAAF internet website. Both documents outline the process by which internet presences can use the crest and official corporate identity of the RAAF and register associations' websites and websites for bases, units, squadrons and wings listed on the official website (www.airforce.gov.au and raaf.gov.au). However, the documents do not mention social media presences; nor is a list of official RAAF social media sites available on the websites.

Ownership of 'unofficial' Defence presences

The review team identified some pages on social media sites that were clearly unofficial pages used by Defence alumni to remain in contact with old friends and colleagues. Some have content consisting mainly of images that are clearly inappropriate, but it is clear that they are personal pages and do not directly reflect on the behaviour of current service men or women.

As part of a longer term initiative, Defence should develop some educational material and guidelines that can be provided to the administrators of unofficial pages. However, other initiatives recommended by this review are of higher priority in the short term.

Control and management of 'official' social media pages

Neither Defence nor the individual Services could provide a comprehensive list of all 'official' social media pages endorsed by Defence. A comprehensive process is needed to identify and manage such pages.

First, Defence personnel should be required to register all pages currently being used in an official capacity, in order to establish a centralised database. Defence may wish to consider an 'amnesty' period in order to receive as many submissions as possible. This will enable Defence to understand the full scope of currently active pages and content.

Second, anyone who is an administrator of a page should provide their details so that, as resourcing evolves and individuals move into new roles, continuity plans can be established to ensure that the page continues to remain active and be managed according to the rules and obligations set out in the social media policy. Additional training and guidance can be provided to those managing the pages, beyond the educational material provided to Defence personnel more broadly. These individuals may also wish to reignite the previously successful cross-functional social media group, which was able to share information and provided internal support in the effective use of social media by Defence.

Finally, establishing a registry and a level of operational control and management of the 'official' pages endorsed by Defence will ensure the authenticity of the source and content in the eyes of Defence, media and the public.

Content management and approval

Defence maintains rigorous processes for approvals to disperse official information, via Communications and Media Branch, using traditional communication channels. Those processes should be reviewed to determine whether official content being posted in the social media space can be aligned.

Defence should be conscious that most effective social media engagements adopt a much softer and informal conversational tone than the ‘corporate speak’ used in many press releases and media scrums. Moreover, social media are about facilitating a dialogue with users, and constraining their use by over-rigorous content approvals would slow responses and compromise authenticity.

Individuals tasked with resourcing the ‘official’ social media channels need to be highly engaged with public affairs teams to ensure that the overall message is consistent. However, social media use requires flexibility in how messages are ultimately delivered. An editorial board consisting of Communications and Media Branch, Marketing, Recruitment and the social media teams (similar to that used by the British Ministry of Defence) would be beneficial. By meeting regularly, the social media teams could organise an improved content management strategy and facilitate approvals for high-level content updates.

“Well defence should be more adventurous when it comes to social media. Today’s young military generation coming through are more evolved around social media. But in saying that there is OPSEC troubles. So if defence could find a middle ground it would be really good.”

(Anonymous response by Defence member)

Monitoring and evaluation

From a marketing and public affairs perspective, there are three reasons why Defence should be monitoring conversation in the social media: to moderate content, to deliver business value and to identify emerging issues.

Moderation

Monitoring can be used for content moderation that is primarily reactive. Content on a page can be evaluated for comments or imagery that breach OPSEC, violate personal privacy, attack others, or are rude or otherwise inappropriate. Some companies and government agencies even use software to flag and/or delete comments automatically, based on keyword or topic, to supplement manual moderation.

“It could be useful for recruitment into defence, however the use of social media will impose an overhead of staff required to monitor and moderate what appears. This overhead will be imposed on security staff as well, on the same principal as that which is applied to Safebase and posting a guard on the entrance to defence bases.”

(Anonymous response by Defence member)

Just as there are policy guidelines for what can or cannot be said by Defence employees, so too should guidelines be developed for comments posted by the public on Defence pages. Based on those guidelines, the administrator may decide to respond to a post or even delete it. Current Defence presences rely solely on the administrators of the pages to monitor these activities, and the practice is managed on an ad hoc basis.

Some of the official Service pages are being monitored by personnel in their own personal time to ensure that problems do not arise. However, other pages are inconsistently monitored or left open for their followers to manage. This ultimately places the onus on Defence personnel who are participating on the pages to have a comprehensive and thorough understanding of the policy and best practice guidelines for posting and sharing content.

Although there is a high volume of active engagement on the official Facebook pages, the number of problematic posts has remained low and they are dealt with swiftly. During the past 18 months, only three commenters have been blocked from the official RAN Facebook page – two members of the public who continually harassed others using the page and one exserviceman who expressed personal complaints about Defence. The public also enforces ‘netiquette’, policing other contributors when comments are considered to be out of line. Such ad hoc moderation has worked so far, but that is partly because the group is relatively small and self-contained.

That approach to moderation would not be as effective for pages with high numbers of followers, such as the official Army Facebook page. It currently has almost 16 times more followers (at 141,804 likes) than the official Navy Facebook page and a significantly higher number of contributors, making informal monitoring more time consuming, resource intensive and probably inconsistent.

Delivering business value

Another reason to monitor social media is to ensure that they are delivering business value and achieving Defence’s key performance indicators for the media. As noted in Section 3.1 of this report, Defence has yet to identify and communicate the strategic purpose of using social media, so measurements have been limited to the volume of fans, the frequency of page visits and a few other metrics. Although those measures provide data, the data does not necessarily translate into robust and valuable insights that can be used to further the business case for using social media. Moreover, many results reported to the senior leadership of Defence do not provide significant value.

There is some circularity in arguments used in the business case for social media and Defence. For example, those administering websites and forums commented that they need more resourcing and formal recognition of their roles. At the moment, they are not effectively resourced and lack the expertise to collect data that supports a business case based on the value of the investment, which might in turn support their arguments for increased resourcing and formal status.

Such an obvious tension can lead to inertia. If Defence could define more thoroughly why, when and how the organisation uses and should use social media, the teams administering the pages would be able to provide more robust metrics and insights to senior leadership and enable best practice sharing. All the participants in these roles would benefit from a longer term project to determine the best allocation of resources to obtain the best value for money and to support best practice.

Proactive conversation identification

Proactive monitoring of social media to identify trends and topics that are relevant to Defence could help the Communications and Media Branch to develop media opportunities. Defence could identify threads of conversation or interests that are important to the general public. That would enable the organisation to allow the public and its interests to drive PR initiatives and ultimately 'shift the conversation' by addressing negative issues quickly and by identifying the types of information and content that engage people positively.

Stakeholder management

In the current operational structure, the Services' pages are very individual. There is limited sharing of content or best practice between Services. To achieve the maximum benefit, Defence should improve knowledge sharing among the Services and include a more robust assessment of social media activities. Changing the culture and attitudes to the use of social media will take time, but the change will be much more palatable for senior leadership and commanders if they are involved in sharing information. This could include simple case studies to demonstrate which activities are most or least effective.

Facebook and Twitter limit access to historical content, so Defence should be documenting its campaigns as well as new initiatives. Those examples could then be used to reinforce policy and education and to improve stakeholder management within Defence.

3.3.3 Discussion

Recent events have resulted in heightened sensitivity about the use of social media. Clearer policies, guidelines and education would mitigate the current risks associated with these channels. By managing both the channels and personnel appropriately, Defence will avoid being placed in a position where the only way forward is to impose greater control on the personal use of social media, which would potentially eliminate a valuable channel for communicating with members and the community.

Although the terms ‘common sense’ and ‘professional judgement’ as applied to social media use need to be clarified, Defence should not discount the fact that most personnel conduct themselves in a manner that is aligned with Defence’s and the Services’ values and expected behaviours. It is also important to recognise that the individuals managing official social media channels on behalf of Defence have tried to use them to improve the reputation and authenticity of Defence brands. From a marketing and communications perspective, there have been very few examples of undesirable content or behaviour. The social media teams and their sponsors have taken the initiative to clear a new path with great potential.

Brand

The international consensus is that military organisations can leverage their brands using social media, for example by engaging directly with stakeholders and shaping public conversation. Research for this review revealed general support and recognition at all levels of Defence for the opportunities that social media provide. Senior leaders recognise the potential benefits, but are also realistic about the risks of social media use by their personnel.

Research also showed goodwill towards and pride in the Defence brands among the Defence community and the public in general. However, the actions of a few have undermined and reflected poorly on the broader Defence brand and community. This is no doubt a reaction fuelled by hypersensitive media concerns about organisations whose work is held in such high esteem by the Australian community.

Defence may wish to expand training to include basic education about brands and marketing, and should consider providing branding tools, such as logos and writing style guides. While it is not possible or advisable to empower all Defence personnel as brand advocates (as the US armed forces have done), consistent resources, guidelines and support mechanisms should be established to empower social media and PR staff to represent Defence in a timely, accurate and effective manner in social media.

Recruitment campaigns are inextricably linked with the Defence brands, and the public sees the social media as roads to recruitment, so action should be taken to align the branding efforts of Defence’s social media teams and Defence Force Recruiting. Previous alignments have resulted in benefits for both parties – engagement and enquiries for Recruiting and a marked increase in followers for the Service presences.

Public relations

PR problems can escalate rapidly in the social media, which provides Defence with significant PR challenges, but also opportunities. Although recent events have resulted in greater sensitivity about social media, clearer policies, guidelines and education could mitigate current PR risks. Instead of attempting to totally control personal and professional social media use (which is extremely problematic and perhaps impossible), Defence should educate personnel in how to respond (or not respond) to certain types of issues (for example, by using a response assessment tree) and how to escalate a response, if appropriate. This will help to ensure that the valuable community engagement enabled by social media will not be lost because of a PR problem.

A further PR challenge for Defence is that the traditional media currently drive most stories, leaving Defence on the margins. To mitigate this, Defence should consider increasing its use of social media to communicate directly with the public, without journalistic interpretation and potential bias. This would allow a more genuine and human tone, a more rapid sharing of information, and the capture of new audiences while meeting obligations to the existing ones.

International best practice shows that social media must be integrated into overall communications strategies, including PR strategies. As well, official social media personnel need to be highly engaged with Defence's Communications and Media Branch, so that critical information can be shared between groups and overall messages are aligned. For example, trends picked up in social media monitoring can be fed into the Communication and Media Branch, which can then prescribe social media content to cater to or exploit those trends.

Official/unofficial presences

Official and unofficial Defence social media presences are not always easily distinguishable. Therefore, Defence personnel should be required to register all social media presences currently being used officially in order to establish a centralised database, in a similar way to the US defence forces. Furthermore, the administrators of those sites should provide their details so that, as resourcing evolves, continuity plans can be established to ensure that the pages continue to remain active and managed. The people managing official social media channels on behalf of Defence have tried to improve the legitimacy and authenticity of the Defence brand, but policy and procedures are needed to ensure the ongoing effectiveness of the channels.

The review found that, on the whole, it is the unofficial pages that have inappropriate content (mainly images), although most of those pages are more personal than official sites and do not directly reflect on the behaviour of current service men or women.

Although it is not possible to control the establishment of unofficial sites, Defence may wish to develop some educational material and suggested guidelines for administrators of unofficial pages that are deemed to have some affiliation with the organisation.

If possible, all social media presences (official or unofficial, affiliated or not) should be monitored for content.

Content management

In social media, content is often referred to as ‘king’. In other words, interesting and accurate content will drive the interest of target audiences. Therefore, it is essential that Defence take a strategic approach to content generation and management on its social media sites. As shown by international best practice, social media content should be governed by content strategies that are aligned with other marketing activities, target audiences and the overall brand.

Good content can be generated from various stimuli (such as events), and should include rich photo and video material. Defence should consider how it could leverage events in its operational and marketing calendar to increase social media audiences, who may then share that content with their networks.

Defence maintains rigorous processes for the approval of official information for use in traditional communication channels by Communications and Media Branch and Marketing. Those processes should be reviewed to determine whether official content being posted in the social media space can be aligned. Most effective social media engagements adopt a soft and informal conversational tone, so that should also be an aim.

Monitoring and evaluation

Monitoring of social media could offer Defence a number of benefits. First, it could be used for content moderation, which although reactive can prevent unwanted information or opinions remaining in the public view for long periods. At a basic level, moderators should identify comments or imagery that could be construed as breaches of OPSEC or personal privacy, are personal attacks or are rude or inappropriate, and advise or escalate the issue as appropriate. Second, monitoring can help Defence understand whether it is meeting its key performance indicators for the channel. Third, proactive monitoring of social media can help to identify trends and topics that are relevant to Defence and important to the public, after which that information could be fed into brand, marketing, PR and content strategy.

STRATEGY AND IMPLEMENTATION

4.1 INTRODUCTION

This report presents case studies and examples from international best practice, showcasing positive, successful social media strategies and their implementation. The United States has invested significant resources into the area, including further funding in 2012 for cyberinitiatives, including social media communication, marketing and engagement. In contrast, the defence forces of the United Kingdom, Canada and New Zealand have opted to take a slower and more cautious approach to social media. While the size of the United States' population could be one reason for its greater engagement in the social media space, another is its desire to be at the forefront of all military technologies.

The core values of a society and the laws governing the rights of its citizens necessarily inform its outlook on social media. The United States has a constitution that explicitly enshrines many personal freedoms, whereas the other countries reviewed here (as well as Australia) have less formally defined personal rights. The United States feels that it has obligations to give and encourage access to instruments that promote free speech, including social media.

Despite the heavy emphasis in this report on policies and practices from the United States (and the US military's domination of offshore best practice examples), US strategies are tailored to meet challenges and demands that differ from those facing the Australian armed forces. Before embarking on any social media planning, strategy or policy development, Defence as an organisation should ask and answer the simple question, 'Why should Defence and its brands use social media?'

It is clear from Australians' high use of social media that those channels cannot and should not be ignored. However, why Australia would follow the lead of the United States when the goals and values of our military forces are different is not so clear. Much can be learned from the US forces' implementation of procedures and their production and management of content strategy and policy documentation, but for Australia to do what is best for its citizens and military personnel Defence must evaluate the importance of social media and the organisational goals that they can help to achieve. After that, Defence will be able to 'cherrypick' from international experience to fashion an approach ideally suited to Australia.

It is easy for social media advocates within Defence to become envious of the resources available to the US armed forces for general cyber and specific social media initiatives, but comparisons should consider the unique objectives and values of each country. Using the United States' social media standards, values and initiatives as a basis for comparison, the questions set out in Table 4.1 can help to clarify the goals of Defence and how they can be achieved using social media.

What?	<p>What are the organisational or campaign goal and key performance indicators?</p> <p>What other channels are being used to achieve the goal?</p> <p>What is the budget or resource allocation for the campaign?</p> <p>What are the Defence's legal (public and employee) obligations in this space?</p>
Who?	<p>Who is trying to achieve the goal?</p> <p>Who is the audience for the campaign?</p> <p>Who should engage with the public on behalf of Defence?</p>
Why?	<p>Why is this goal important?</p> <p>Why is social media the right channel for the campaign?</p>
When?	<p>When should the goal be achieved?</p> <p>When will the campaign/communication begin and end?</p>
Where?	<p>Where is the goal? (A country? Online?)</p> <p>Where will the social media strategy be implemented?</p>
How?	<p>How will the goal be achieved?</p> <p>How will the strategy be implemented?</p> <p>How will it be monitored?</p> <p>How does Defence keep up with technology and cultural progress without spending significant resources on continually learning new technologies?</p> <p>How can individuals interested in military topics be grouped and marketed to efficiently?</p>

Table 4.1: Clarifying goals for social media

This review shows that there are pockets of highly effective social media practice and guidelines in the Services. However, it has been acknowledged at all levels that a centralised approach to social media strategy, policy and governance is required. Defence's work not only in the social media, but also in the overall digital space, lacks clear strategy, policy and governance.

Therefore, Defence should consider establishing the proposed Digital Executive Oversight Committee (DEOC), headed by a senior social media adviser. DEOC would provide executive sponsorship and guidance to ensure that the Services' strategies and tactics are aligned with broader Defence business objectives. The committee should have balanced representation from across the Services and include the Ministerial and Executive Coordination and Communications Division and CIO Group, Personnel Strategies and Policy Group, Defence Community Organisation and Intelligence and Security Group. DEOC should ensure that social media practice is strategically linked with the overall mission and objectives of Defence. Even though strategy and direction would be centralised, resourcing should remain locally based, in order to address the unique needs of the individual Services and ensure responsiveness.

A centralised and coordinated understanding of how Defence, and specifically the Services, will use social media is crucial to ensure successful and appropriate use of the channels. That understanding will affect the development of policy and the use of social media for professional and personal purposes by Defence personnel. A coordinated approach to the high-level components will be extremely important to ensure that the Navy, Army and Air Force and the Department of Defence can each use social media appropriately as they see fit. While each of the Services has a wide variety of requirements and its use of the channels will vary, its activities should ultimately align with the core strategic principles set out centrally.

Any attempt by Defence to coordinate all social media centrally runs the risk of creating approval bottlenecks, which could reduce the speed and authenticity of the conversation and engagement. Organising social media requires a hybrid approach to management: top-down leadership should influence medium- and long-term strategy and policy, but day-to-day management should be decentralised.

DEOC should set out high-level guidance defining unofficial and official use of social media. The committee should also define the depth of Defence's social media policy as it relates to both professional and personal use, be it on base, off base, within the Defence Restricted Network, in Defence housing, or when deployed. DEOC members will be required to invest considerable attention over the short term. However, once the channel strategies, policies and operational controls have been finalised, the committee should only be required to meet 4–6 times a year to monitor performance and understand the changing landscape.

The proposed structure would also support centralised expenditure for incremental resources such as monitoring and moderation. In addition, the committee would support visible executive sponsorship of social media in Defence.

4.1.1 Strategy management

The suggested strategy governs the overall social media approach by Defence and aims to involve senior personnel in communications strategies. Each of the Services has already set out its organisational goals and values, so this process is designed to ensure that social media and digital technologies are governed by robust policies that support them. The process diagrams in Figure 4.1 and Figure 4.2 are intended to provoke discussion. Each stage will need to be clearly defined and controlled by Defence to ensure stakeholder acceptance.

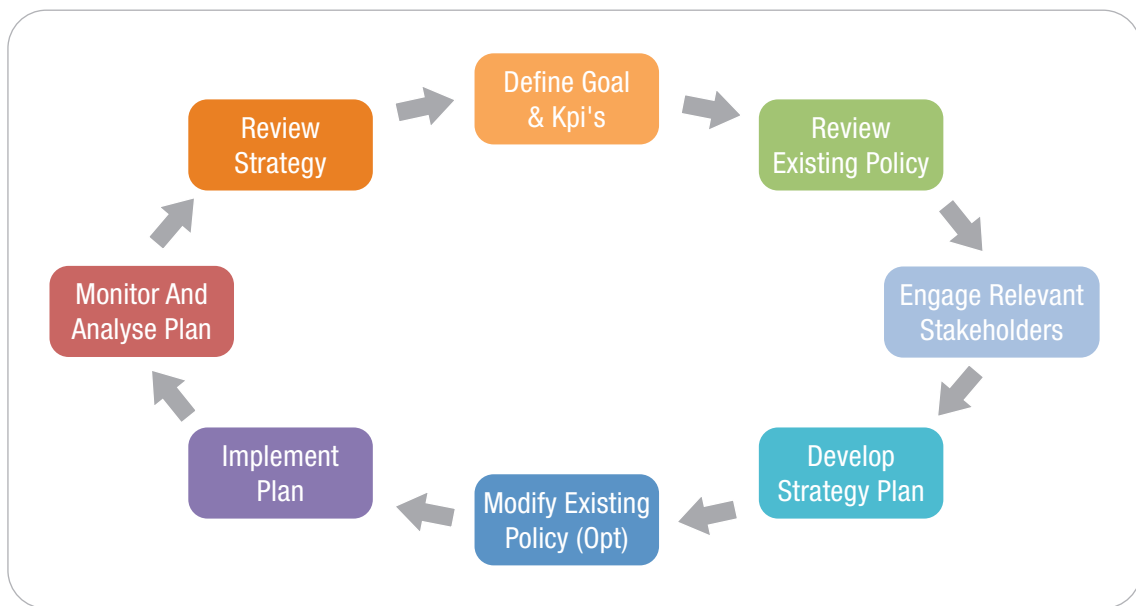


Figure 4.1: Strategy management process

4.1.2 Campaign strategy

The suggested campaigns or initiatives follow the same process, without the option of adjusting policy, with the expectation that clear metrics will be available to measure the results of each campaign. This process involves stakeholder engagement with subject matter experts to produce engaging content that meets the goals of the organisation and the campaign (Figure 4.2).

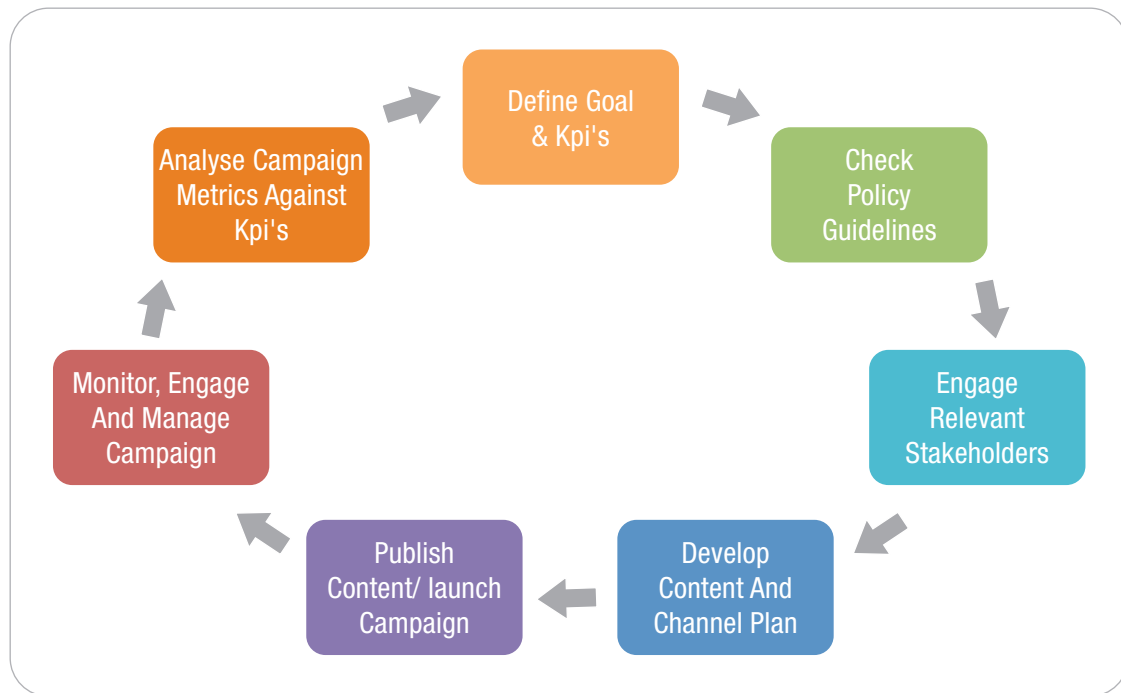


Figure 4.2: Campaign strategy process

4.1.3 Goals and objectives

The ‘crawl, walk, run, fly’ concept is often used in business to describe the growth and launch process, either of the organisation or of a particular strategy within the organisation. Those stages can be applied to Defence’s social media marketing and engagement goals. The first three steps (crawl, walk and run) are applied to all organisational and campaign initiatives, while the final step (fly) is the implementation of a crisis plan when the need is identified (for details, see Figure 4.3 and Table 4.2).

A communications crisis plan must be a part of the overall communications strategy. Planning and education should be designed to give responsibility to those who need it in order to communicate in the space with the required speed and efficiency. The crisis plan, or ‘flying’, cannot continue indefinitely and is only used to manage specific sets of predefined issues.

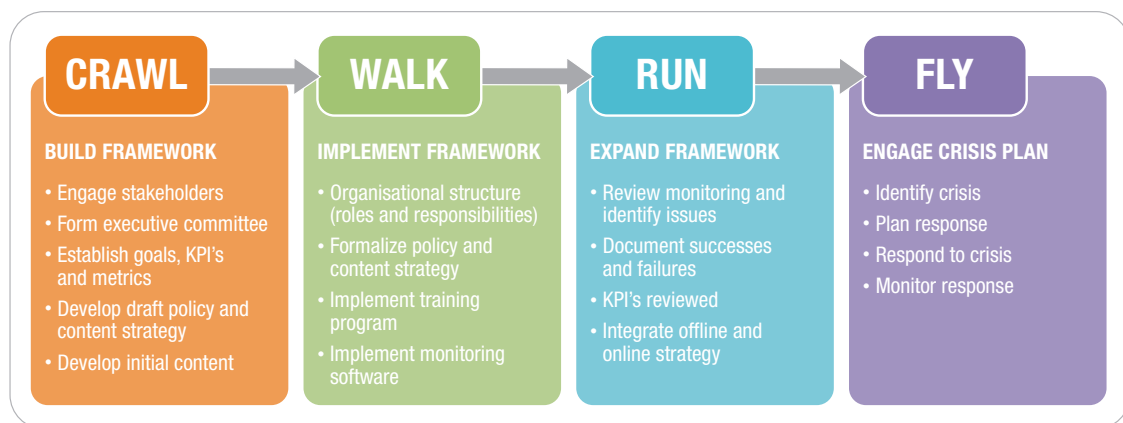


Table 4.2: Steps in the ‘crawl, walk, run, fly’ implementation strategy

Based on the findings of this review, the various Defence social media initiatives range from crawling to taking their first tentative steps. These initiatives have an established framework of social media sites with teams in place to deliver content and engage visitors. While they are in need of some organisational refinement as documented in this report, that work is currently underway.

4.1.4 Australian Defence Force mission statements

Table 4.3 shows Defence mission statements and how they might be translated into goals for social media.

Mission statement	Social media goals
<u>Australian Army.</u> The Australian Army's mission is to provide a potent, versatile and modern Army to promote the security of Australia and to protect its people and interests.	<ul style="list-style-type: none"> • Communicate message/image of a potent, versatile and modern army. • Increase and engage potential recruits and create a dialogue that may lead them to join. • Engage friends and families of personnel to maintain Defence community welfare.
<u>Royal Australian Air Force</u> The Royal Australian Air Force (RAAF) provides air and space power for Australia's security. It is the youngest of the three armed Services in the Australian Defence Force (ADF) but the second-oldest air force in the world.	<ul style="list-style-type: none"> • Communicate message/image of the RAAF. • Increase and engage potential recruits and create a dialogue that may lead them to join. • Engage friends and families of personnel to maintain Defence community welfare.
<u>Royal Australian Navy.</u> The Navy's role is to promote and protect Australia's interests at sea using a mix of ships, submarines and aircraft manned by highly trained and skilled personnel and equipped with appropriate sensors and weapons systems.	<ul style="list-style-type: none"> • Communicate message/image of protection, highly trained personnel and superior equipment. • Increase and engage potential recruits and create a dialogue that may lead them to join. • Engage friends and families of personnel to maintain Defence community welfare.
<u>Defence Jobs.</u> The Defence Jobs website provides detailed information on all Navy, Army and Air Force careers. You can search for jobs, access online services or register for My H.Q. — a secure web site where you can make an online application.	<ul style="list-style-type: none"> • Increase and engage potential recruits and create a dialogue that may lead them to join. • Maintain an engaged audience for broadcast communications and campaigns.
<u>Defence recruitment centre – overseas applicants</u> Defence is looking for serving or ex-serving foreign military personnel, who can directly transfer their job and life skills to whatever Service they join. If you are not an Australian Citizen or Permanent Resident, you may still be eligible for entry into the Australian Navy, Army or Air Force.	<ul style="list-style-type: none"> • Seek out former foreign military personnel and engage them in dialogue about Defence. • Harness the skills of trained, experienced service members.

Mission statement	Social media goals
<u>Defence Reserves Support</u> The Defence Reserves Support provides a link between the Australian Defence Force (ADF), employers and the community from which Reservists are drawn. This site provides information for both reservists and their employers. It includes information about the Reserves and recruiting information for those wishing to join.	<ul style="list-style-type: none"> • Increase and engage potential recruits and create a dialogue that may lead them to join Defence. • Maintain an engaged audience for broadcast communications and campaigns.
<u>Defence Signals Directorate.</u> The Defence Signals Directorate is Australia's national authority for signals intelligence and information security.	This subject is likely not to be suitable for social media.
<u>Directorate of Oceanography and Meteorology</u> The website of the Royal Australian Navy's Hydrographic Meteorological and Oceanographic Group, which provides maritime geospatial information and services to meet Defence requirements and national obligations. METOC consists of four sections: Operational METOC Centre; Nowra Weather and Oceanography Centre; Ocean Data Services; and METOC Geospatial Services.	<ul style="list-style-type: none"> • Educate stakeholders about the services provided by the directorate. • Provide a contact and content point for potential media research. • Promote the work of the directorate through positive, popular and unique content, such as photos.
<u>Global operations - Australian Defence Force</u> The global operations page for the Australian Government Department of Defence provides information relating to global operations that Australian Defence Force personnel are currently involved in.	<ul style="list-style-type: none"> • Provide information to media and communities about global operations.
<u>Royal Australian Air Force Multimedia Site</u> The Royal Australian Air Force multimedia site includes video clips, video downloads, podcasts, games, images, childrens resources, interactives and kids media.	<ul style="list-style-type: none"> • Communicate message/image of the RAAF. • Increase engagement with existing content through sharing.

Table 4.3: Defence/ADF mission statements – social media goal comparisons

(Source: <http://australia.gov.au/topics/defence-and-international/australian-defence-force-adf>)

4.1.5 Moderation

A balance needs to be struck between allowing individuals to express their opinions and protecting the community from offensive behaviour or postings. Moderation is the manual or automatic process for assessing and possibly removing such material. Clear guidelines should be posted to the channel where communication occurs, so that contributors are aware of their obligations. Software is available to automate moderation for basic breaches, such as the use of profanities. However, human behaviour in social media is best monitored by other humans, rather than by software.

Moderation is not the removal of opinions or ideas that contradict an official line, which would be considered censorship in the social media. It is the removal of material considered to be extreme and offensive by the majority of the contributing community. What is acceptable in one community may not be acceptable in another. Boundaries are defined by a combination of the community members, the site administrator, the brand and the mechanics or site used for the interaction.

The following material is generally moderated from commercial or government websites or social media channels:

- profanities (at an age-appropriate level for the audience)
- abuse and personal attacks
- hate and discrimination
- obscenity
- personally identifying information.

Additional information that should be moderated for Defence includes:

- security breaches
- breaches of the general code of conduct
- incorrect information.

4.1.6 Monitoring

Monitoring has four primary purposes:

- to identify content that is considered a security breach or requires moderation
- to gather statistics in order to measure the success of a campaign or piece of content
- early identification of potential crises
- brand and subject trend identification and analysis.

In order to moderate significant volumes of conversation, Defence should develop a monitoring process that uses a combination of social media monitoring software and human analysis. The process will depend on the overall goals of Defence's social media strategy and the individual KPIs of each of the commands and owners of social media presences. The owners should be responsible for their own monitoring and moderation, but too much latitude would create inconsistencies in data collection and make it difficult to compare initiatives accurately. The monitoring process should be standardised across all of the Services to allow direct comparisons and analyses, and conducted at either senior level or by coordinators under the direction of the senior social media adviser.

4.1.7 Branding

Branding is a proactive process that starts with the 'Plan' phase (Figure 4.4).

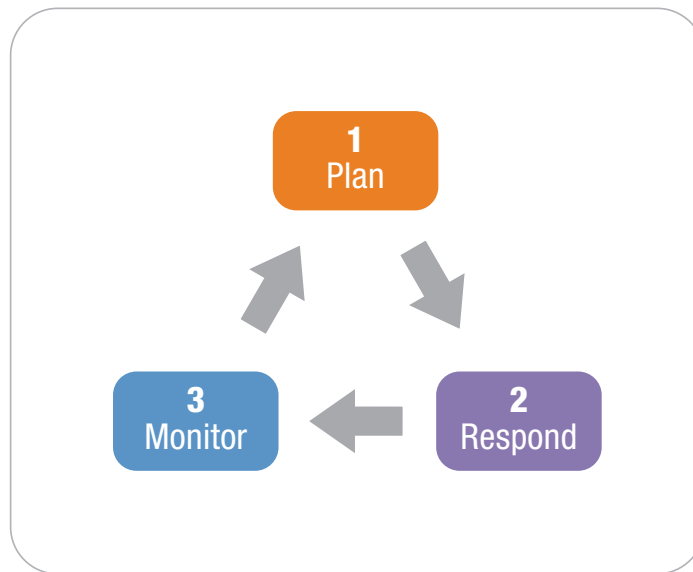


Figure 4.4: Branding – proactive process

4.1.8 Crisis management

Crisis management is a reactive process that starts with the identification of the crisis (Figure 4.5).

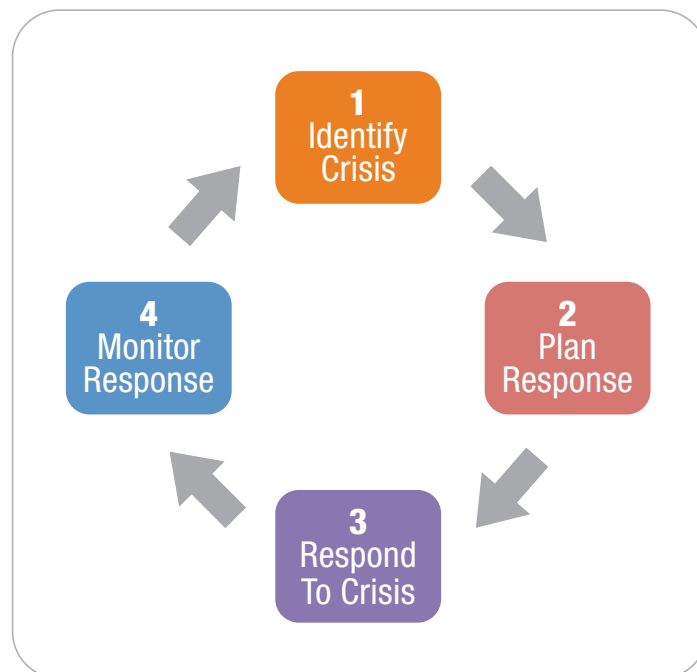


Figure 4.5: Crisis management – a reactive process

4.1.9 Channel strategy

Defence currently uses social media only in what it considers to be ‘safe spaces’. Those spaces are usually online networks frequented by families and are by nature supportive. Each of the Services is having some success in social media, but they lack clearly defined goals, consistent reporting methods and internal promotion of achievements, causing their efforts to go mostly unnoticed. When considering a channel, it is important to consider how the channel can be monitored, moderated and analysed to ensure that it is meeting defined KPIs.

A social media channel strategy should not be developed as a stand-alone plan. The choice of channel must take into consideration both the channel’s ability to achieve a goal on its own and its ability to complement and support other digital or traditional media channels. It is logical to select a social network with the most members in the target demographic. Currently, for Defence, that would most likely be Facebook, but individual communications may be better suited to other channels such as blogs, forums or Twitter, depending on the goal of the communication.

Questions to ask before selecting a channel include the following:

- Does my goal require two-way communication and audience participation? Why?
- Can the message be communicated using short form text (microblogging)?
- Which other channels are being used to achieve the goals?
- What content (and content types) will be published for the campaign/communication?

4.2 BRANDING STRATEGY

4.2.1 Brand health

The review team used BrandAsset Valuator (BAV) to better understand the current 'health' of the Defence brands.

BAV is Young & Rubicam's proprietary research tool, and is the largest database of consumer opinions in the world and a rich source of brand intelligence in Australia.

An annual Australian online survey of 1,000+ questions undertaken by 2,500+ consumers provides access to:

- 25 million brand facts
- information for 1,200+ consumer brands in 110+ categories
- 58 exclusive brand metrics
- 17 years of continuous tracking to date
- annual data refreshment and category definition for subscribing clients.

Data from BAV, shown in Figure 4.6 and Figure 4.7, demonstrates that a wave of negativity in popular media about Defence issues is out of step with the sentiments of the general public. Each of the Services ranks in the top 6th percentile of all brands in BAV, making the Defence category second only to the Australian Emergency Services category (ambulance, fire brigade, police and SES).

The Navy, Army and Air Force are some of the most liked, even loved, brands in Australia, and all three have gained in all aspects since the 2009 BAV survey (Table 4.4).

In the future, this type of information should be sourced, tracked and where appropriate communicated internally to Defence members. Many members consume journalistic content and accept that it reflects the opinion of the community in general. Qualitative and quantitative research shows that this can cause a misplaced belief that Defence is losing the support of the public. This review suggests that such a notion should be challenged.

To date, BAV has not included government departments in its research, so similar reporting was not available for the Department of Defence. The department is to be included in 2011 research yet to be undertaken.

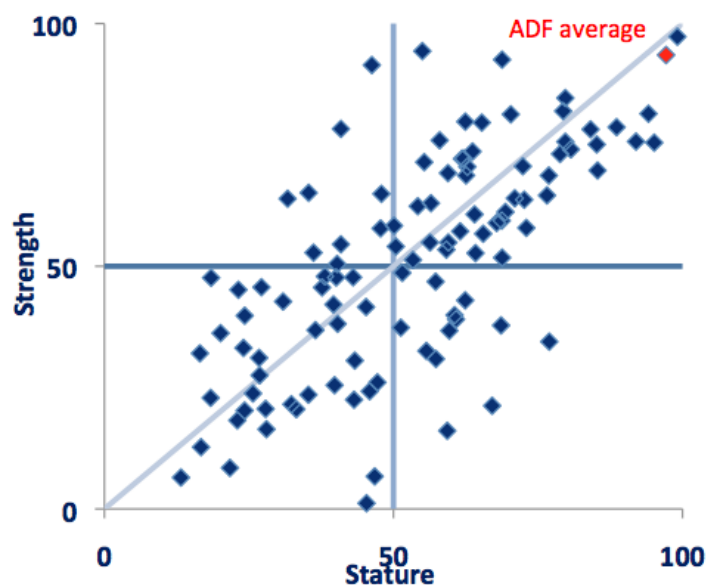


Figure 4.6: BAV 2010 powergrid – all category averages, all brands, all adults

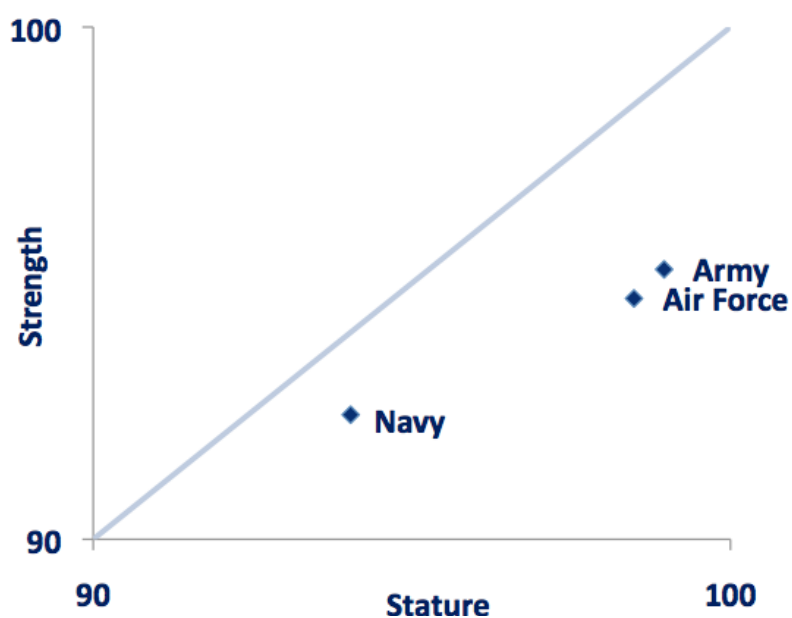


Figure 4.7: Breakdown of Services within the power grid (note the scale)

(Source: BAV 2010, Australia – all adults)

	BrandAsset score ^a	Overall position in 2010 BAV brandscape (1,061 brands)	Esteem score in 2010 BAV brandscape (1,061 brands)	Esteem position in 2010 BAV brandscape (1,061 brands)
Navy	94.61	58	98.58	16
Army	98.20	20	99.62	4
Air Force	98.01	22	99.72	5

Table 4.4: BrandAsset scores for Navy, Army and Air Force

^a BrandAsset score is an overall rating that combines levels of brand strength and stature. It indicates overall performance of the brand ranked against all brands in the BAV brandscape.

4.2.2 Employer brand

Many public sector organisations and businesses struggle to establish meaningful brand values because their employees see their brand as the domain of marketing and sales departments. For some, brand is reduced to a clever line or a logo. Defence suffers from no such problem, as brand values are at the core of the organisation. The brands' inherent values are taught from the point of induction and are the mainstay of education and delivery throughout an individual's journey through Defence. ADFA cadets refer to brand values as if they have known them from birth.

Brands are, by their nature and through the consistent delivery of experiences, a short cut to underlying values. Over time, people come to understand the experience they should expect from any given brand.

Defence has a clear set of brand values:

Professionalism, Loyalty, Integrity, Courage, Innovation, Teamwork

In turn, each of the Services has a set of values specific to its own culture and needs:

- **Navy** – *Honour, Honesty, Courage, Integrity and Loyalty*
- **Army** – *Courage, Initiative and Teamwork*
- **Air Force** – *(from vision) One team – Swift, Decisive, Resilient and Respected*

The representation of the brand values in official social media is essential to ensure that the brand remains consistent. Social media guidelines for Defence members should also refer to the values; while some will be more pertinent than others, all should be considered as part of the process.

There are no better brand advocates and ambassadors than an organisation's committed members. This is a branding truth that has already been recognised for some time throughout Defence and during campaign development, well before the advent of social media. Throughout social media engagement, the 'power' of Defence people is enabling Defence brands to deliver, in the words of one member, 'our story, our way', to great effect.

Using members as brand ambassadors has the added advantage of helping to create a desirable employer brand. This form of branding should aim to attract and inspire potential recruits and their parents and friends. Nevertheless, the employer brand is delivered through actions and behaviour, not through endorsed communications in official channels, which should be left to the PR and communications teams.

While the review team was given the task of defining a brand strategy to enable the enhancement of Defence's brands in social media, the brand direction of 'people first' currently being used is the ideal method for engaging in social media. The review recommends that the pursuit of this underlying principle continue unchanged.

One noteworthy challenge of this branding method is that, if members are placed at the centre of a communications strategy, any negative action by any members of the group will inevitably reflect more strongly on the brand – a reality that could be said to be true for Defence in recent months. The challenge can be compounded by one of the main social media phenomena affecting society (businesses, governments and Defence alike): the blurring between the personal and the professional identities of individuals and the organisations they may represent. The personal identity of a user is now published online in an easily sharable format, and younger people view privacy as a value differently from the generations who preceded them. This increase in online content sharing means that the personal qualities, habits and activities of an individual can reflect on their employer, sometimes generating a negative brand image.

4.2.3 Channel ownership

The desire of individuals to sculpt their identities in social media drives many to connect with and promote subjects that interest them and help to define their identity in their networks. This structuring of identity can sometimes lead to individuals creating pages or profiles for organisations they participate with, often without support or approval from the organisation. It can be said that if an organisation does not create its own official channel, someone else may create an unofficial one. The unofficial channel may generate engagement with the organisation's audience that does not complement and may even conflict with the official message in other channels.

The idea that some control over content and message is better than no control at all inspires many organisations to reluctantly create presences in social media.

It can be argued that if an unofficial page is building engagement with an audience, the audience wanted to engage with that brand in the first place. The real owner of the brand may miss a valuable opportunity to connect. Unofficial presences, particularly in areas with controversial messages and strong 'for' and 'against' audiences, can be damaging to the reputation of the organisation's brand.

The Navy, Army and Air Force publicise their official channels on their official websites. However, research revealed dozens of associated sub-brand Facebook pages for Defence. It is unclear whether those pages are official, unofficial, official/unofficial or unofficial/official – all terms used by Defence staff to describe them. The volume of sub-brand sites is likely to result in an inconsistent brand experience being communicated to the community.

This labelling issue demonstrates a level of confusion among Service members. In addition to other reasons, Defence members have indicated that they started Facebook pages and other social media presences to bypass what is described as a slow and heavily governed process for publishing content to the official Defence websites. It is also true that the official websites attract different audiences and therefore social media offers extended communication reach. However, if social media become the channels of choice for Defence communicators, it is possible that an increasingly poor experience will be delivered to the users of the official websites.

It is important to note that the identity of Defence as a brand is not on the whole a social identity. With the exception of some specific events, the organisation does not usually promote social activities to outside communities; nor does it have a requirement to encourage day-to-day engagement with the general public about its activities. The goals of Defence are, in many ways, contradictory to the traditions of social media, where openness and transparency are often considered more important than security and confidentiality. Defence should see social media as tools to achieve many goals, not as an obligation to create a 'social defence force' at the potential cost of security.

4.2.4 Brand assets

A positive and consistent brand representation can benefit the organisation not only through creating a sense of trust in the sites and content being viewed, but also by establishing consistency across sites covering different subjects that are clearly identifiable within a single brand family.

In traditional media, communications and marketing teams are usually responsible for the brand imagery of an organisation – a consistent look and feel using mechanics such as language, logos, graphics, colours and images.

A potential brand control would be to provide a resources section for relevant Defence staff on official websites, or intranets with logos and pre-designed social media graphics (such as Facebook skyscraper profile banners). This content would be displayed with clear instructions for its use and details of its copyright restraints. Potentially, the inclusion of 'social media ready' logos on the Department of Defence's Australian Defence Image Library website would satisfy this requirement; however, this review has not investigated the governance of the site.

Defence may wish to develop a process by which members and the general public can report potential copyright infringement and unauthorised uses of brand image mechanics in social media. Defence could then consider reporting infringements to the channel owners or administrators and asking for the offending materials to be removed.

4.2.5 Recruitment branding

Social media provide an obvious way to engage potential recruits with content that represents the values of the individual Services or Defence as a whole.

Understandably, many potential recruits are drawn towards the three Service brands and attempt to engage with the Services and their members in the social media environment. The demographic profile of social media users, the platform and in many cases the content being delivered contribute greatly to recruitment. Then again, due to the organisational structure and in some cases the beliefs of Defence and Defence Force Recruiting, many potential recruits are being redirected to Defence Force Recruiting's own website or phone number. This is understandable and is intended to ensure that the potential recruit receives the best advice possible. However, from a brand perspective it can seem slightly dismissive, and not only for the individual – the redirection is often posted publicly and is visible to the wider online community.

A number of activities that engage potential recruits via official Defence social media sites have been conducted. While those activities are covered elsewhere in this document, it is worth noting that the engagement was highly effective and produced many 'likes' for the pages. In social media, 'likes' are a brand currency for future communication.

4.2.6 'Test and learn'

Defence should implement an internal process for documenting and promoting the outcomes of social media activities to its social media stakeholders. This would counter negativity towards the use of social media, but also improve on the 'test and learn' culture. For many organisations, test and learn methodology can deliver meaningful insights into the use of social media for their brands. If there is no proper documentation of achievements (and failures), the real benefits of such factors as effort and cost reduction are not easily realised.

4.2.7 Department of Defence – a different brand?

Governments and their departments regularly receive negative comments about policy development and service management. This is partly due to competition between social groups.

The Department of Defence as a government body should consider its approach to official social media differently from the individual brands of the Navy, Army and Air Force. For example, department staff may want to engage members of the Defence community and the public in open forums to discuss issues such as the development of policy. With that type of engagement in mind, Defence should consider the resources required, the ability of the community to use the online environment to voice alternative opinions, and whether such a strategy supports the overall goals of Defence. It may well be that the current practice of using the department's official website (rather than social media) best suits its role and needs.

The branding needs of the Department of Defence will ultimately require a much larger consideration of overall Australian Government needs and directions, and so have been considered out of scope for this review.

4.2.8 Point of failure – reliance on individuals

Defence employees in communications roles are driven to monitor social media manually, in their own time. Their commitment is likely to be unnoticed, despite the significant value it provides to the organisational brands. One concern of the review team is that this creates ‘single points of failure’ –when a person leaves a position, an entire communications channel is left unattended, with a detrimental effect on the brand.

This voluntary service has also created an expectation of service after hours. Contributors expect responses to posts within minutes or hours, not days or weeks as existing approval processes require. Defence will need to define its commitment to this ‘always on’ aspect of social media. The commitment is currently defined by the need to moderate content, not the need to engage with users.

4.2.9 Content strategy

In social media, content is at the core of all activity. Discussions, promotions, photos, articles, links and so on are all content, without which social media would simply be called ‘chat’ or ‘communication’. The act of sharing creates the ‘social’, and content (or information) creates the ‘media’.

Content is the tool with which the unengaged can be reached via the engaged. That is, those who are already engaging with the content can attract those who are not by sharing the content in their own networks. The engaged (Tier 1) audience is likely to be very interested in the content or subject, and in the case of Defence is likely to comprise staff, family members and other stakeholders. The unengaged (Tier 2) audience comprises their friends and networks who may have some interest in the content or subject once they have seen it.

A social media content strategy can drive interest in offline communications, such as phone or general digital communications (for example, a website). However, even if it is a stand-alone strategy it should still consider other marketing objectives outside social media and ensure that it is complementary – not contradictory.

Ideally, the general content plan would be set by an executive committee and the senior social media or digital adviser in consultation with the communications team for each Service. This ensures that vertical pillars and horizontal topics complement each other, providing a connection between the Services that is not currently seen in social media. For example, the subject of hospitality and catering is relevant for all the Services, and content produced in that area can be used across the vertical pillars (Figure 4.8). In particular, if the Services are looking to recruit chefs, marketing across the three Services to promote that career would not only Defence Force Recruitment to achieve its goals, but would give each of them the opportunity to showcase their own work in that area.










	ARMY	NAVY	RAAF
Engineering			
Science			
Hospitality			
Equipment	Tanks	Ships	Planes
People	Soldiers	Sailors	Pilot

Figure 4.8: Content matrix

Content can be themed daily, in the style of the US Army's fiveday content plan, or through weekly, monthly and annual plans that take into account diarised Service events and give the marketing and communications teams clear guidelines on what is expected of them. Weekly meetings with a social media adviser and the coordinators from each of the Services are opportunities to exchange ideas, identify positive and negative conversations, improve processes and identify potential crises.

The content shown in Figure 4.9 showcases 20 Navy chefs gaining work experience at the ARIA restaurant in Sydney. Matching this type of content with a recruitment drive for hospitality staff would not only help to achieve the recruitment goal, but would be likely to increase morale within Defence hospitality services.

Exciting roles, such as operating guns and planes, are often promoted through content, while seemingly less exciting roles such as cooking food for the troops are given limited exposure and promotion. There are good stories in every area of Defence, and they can be used as content to achieve specific goals and targets for recruitment and other purposes.



Figure 4.9: Navy chefs gaining work experience at the ARIA restaurant in Sydney

(Source: <http://www.facebook.com/media/set/?set=a.252882814726426.79340.123855294295846&type=1>, retrieved 27 July 2011)

4.3 POLICY STRATEGY FRAMEWORK

Once a clear strategic direction for social media has been established for Defence by the executive leadership, policy and governance should be established to reflect the new way forward. Defence (as well as the individual Services) has already begun to develop the necessary policies, guidelines and SOPs. The work of the social media teams can be further enhanced through the establishment of the DEOC, which will be able to review all of the existing documentation to ensure consistency and alignment.

By ensuring that its social media policies are clear and concise, Defence can minimise confusion and ultimately establish confidence and clarity for all Defence personnel. The primary Defence policy addressing elements of social media (*DI(G) ADMIN 08-1*), requires updating to address the complexity of the social media space. This review's best practice and legal obligations audits demonstrate the need to have a social media policy either as a subsection within *DI(G) ADMIN 08-1*, or as a separate policy.

The objective of the new policy is to set bounds for Defence members' use of social media, whether as part of a member's professional responsibilities or in a personal capacity, to limit the risk of damage being caused to the organisation and members by that use. As Stephen von Muenster said in Section 2.2 of this report:

"A properly drafted and enforced Defence social media policy is Defence's most effective risk management tool in protecting the organisation from reputational damage and legal liability from the use of social media in during both professional use and private use."

With clear parameters for appropriate conduct during professional and private uses of social media, personnel can ensure that their online behaviour does not put them in breach of Defence's Values, Code of Conduct or *DI(G) ADMIN 08-1*.

4.3.1 Policy components

Defence should consider the following policy components, which address the complexity of the social media landscape.

Scope of policy

The policy should focus mainly on the human behaviour associated with communicating online or via social media. It should be platform-flexible, as new social media platforms are being launched at a rapid rate. Should Defence limit itself by defining rules by platform, such as Facebook or Twitter, the organisation runs the risk of policies becoming outdated relatively quickly. It is important to ensure that the policy is able to respond to changes in the social media landscape, such as the recent release of Google+. The policy should be updated as required so that it remains relevant, and members need to be made aware of any changes. Additional training may be required as the policy evolves.

Defining channels and use

There is an opportunity to properly define social media policy with reference to three types of channel and their corresponding uses (Figure 4.10).

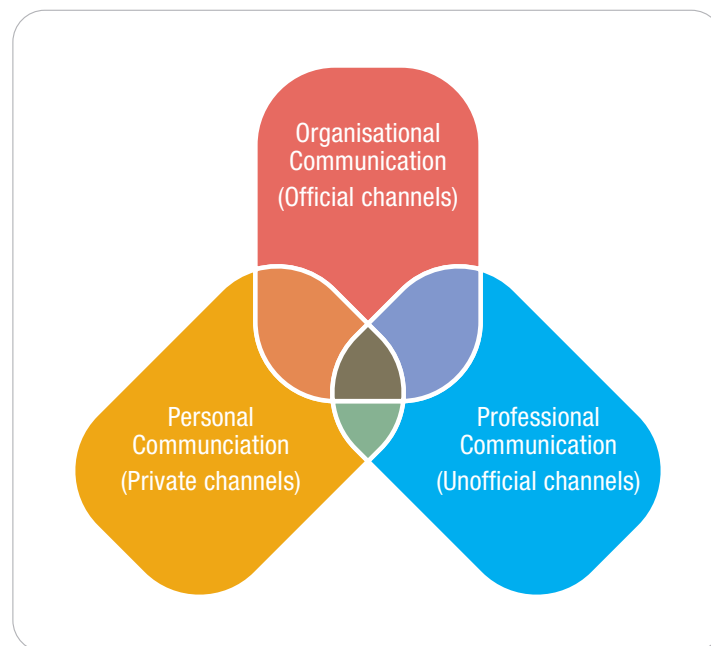


Figure 4.10: The three types of social media channel and their uses

Organisational communication occurs within *official* Defence social media channels, which are channels established and run by Defence, such as the Australian Army Facebook page. Any use of them by Defence personnel constitutes *organisational* communication. These channels should all be listed in the Defence social media registry, and they should be actively monitored and moderated by Defence social media personnel.

Professional communication occurs within *unofficial* channels, but implies affiliation with Defence. These are channels established by individuals or organisations with a vested interest in Australian defence activities, such as Defence veterans or community support groups. Use of these channels by Defence personnel constitutes *professional* communication and imposes greater responsibility on personnel to represent Defence appropriately.

Personal communication occurs within the remaining social media channels (*private* channels). This includes social media channels with no affiliation with Defence. Use of these channels by Defence personnel constitutes *personal* communication. Defence members should neither claim nor imply that they are speaking on behalf of Defence when using private channels. If a member discloses that they are a member of Defence, they must state that their views are their own and not those of Defence.

Although these three types of social media channel and three types of use are the focus of Defence's social media policy, they will never be mutually exclusive. Therefore, the areas where the channels and uses intersect need to be addressed.

Overarching Defence policies and values

To provide context for Defence's social media policies, Defence should inform personnel about rules and regulations that would supersede the Defence social media policy embedded in *DI(G) ADMIN 08-1*. It should remind members to familiarise themselves with their terms of employment and all other applicable Defence policies and instructions, including those covering the escalation of issues and the consequences of policy breaches. These include:

- Legislation
 - *Archives Act, 1983*
 - *Defence Force Discipline Act 1982, section 58*
 - *Public Service Act 1999, section 13*
 - *Privacy Act 1988, section 6*
- Regulation
 - *APS Values and Code of Conduct in practice, Australian Public Service Commission*
 - *Defence security manual, Part 1 – Protective security and Part 2 – Internet content*
- Policy
 - *DI(G) ADMIN 10-6 Use of Defence telephone and computer resources*
 - *DI(G) PERS 35-3 Management and reporting of unacceptable behaviour*
- Guidelines
 - *OPSEC and force preservation awareness training*
 - *Living the Service values*
 - *DIMPI 2/2003 – Hand-held imagery metadata standard and procedures.*

Defence should consider reviewing its level of tolerance for personal use of social media by members during work hours, whether using a personal device or a Defence-owned asset. As a minimum, access to the official Defence sites should be considered. This review has noted that certain technical restrictions on the Defence Restricted Network, such as bandwidth, also affect access to social media sites; that also needs to be taken into consideration.

4.3.2 Policy for personnel who manage 'official' social media

As part of its policy review, Defence should consider personnel who are responsible for the administration and management of official social media sites. They potentially require specific policy considerations in addition to the Defence Restricted Network and the computer assets they need to perform their jobs efficiently.

Authorisation protocols for allowing public comment will need to be reviewed so that administrators of social media are able to respond to posts in good time, mitigating the risks associated with failing to post prompt responses. The protocols should be closely aligned with the social media crisis response procedures.

Defence should also consider reviewing policy to ensure that those tasked with professional communication via social media are considered within policy such as *DI(G) ADMIN 106*.

4.3.3 Social media engagement principles

Social media engagement principles should establish expectations that are not explicitly covered in existing policy, and also demonstrate how existing policy may be interpreted in the social media space. Defence may develop social media policy covering the three categories of social media channels and uses outlined in Section 4.3.1. For the purposes of policy development, professional and personal use may be considered together, recognising that Defence personnel can never fully separate their behaviour in social media from the Defence brand.

The following points, which are informed by the legal obligations audit, should be considered when developing social media policy.

Organisational use of social media

- Only those authorised to comment may do so as representatives of Defence.
- Explain the authorisation process.
- Set out what can and cannot be done, for example:
 - Disclose that you are an employee/contractor of Defence, and use only your own identity or an approved official account or avatar.
 - Disclose and comment only on information classified as public domain information.
 - Ensure that all content published is accurate and not misleading and complies with all relevant Defence policies.
 - Ensure that you are not the first to make an announcement (unless specifically given permission to do so).
 - Comment only on your area of expertise and authority.
 - Ensure that comments are respectful of the community in which you are interacting online.

- Adhere to the terms of use of the social media platform or site, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws, and other Defence policies and guidelines.
- If you are authorised to comment as a Defence representative, you must not:
 - post or respond to material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a court suppression order, or is otherwise unlawful
 - use or disclose any confidential or secure information
 - make any comment or post any material that might otherwise cause damage to the reputation of Defence or bring it into disrepute.
- Set out a moderation policy and approval processes.
- Provide a frequently asked questions section.
- Provide examples of acceptable and unacceptable social media communications.

Professional and private use of social media

- Have a separate set of guidelines (best practice).
- Do not restrict use, but encourage best practice behaviour.
- Provide a frequently asked questions section.
- Provide examples of acceptable and unacceptable social media communications.
For example, state that members must:
 - take responsibility for what they post
 - disclose and discuss only publicly available information
 - ensure that all content published is accurate and not misleading and complies with all relevant Defence policies
 - expressly state on all postings identifying them as Defence members that the stated views are their own and are not those of Defence or the government
 - provide the suggested disclaimer ('The views expressed are mine alone and do not necessarily reflect the views of Defence.')
 - be polite and respectful to all people they interact with
 - adhere to the terms of use of the social media platform or site, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws, and other Defence policies and guidelines.

- State that members must not, for example:
 - post material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a court suppression order, or is otherwise unlawful
 - imply that they are authorised to speak as representatives of Defence or the government, or give the impression that the views they express are those of Defence or the government
 - use their Defence email address or any Defence or government logos or insignia
 - use the identity or likeness of another member or contractor of Defence
 - use or disclose any confidential information or personal information of others obtained in their capacity as Defence members
 - make any comment or post any material that might otherwise cause damage to the reputation of Defence or bring it into disrepute.
- Set out what is reasonable and unreasonable private use and give examples.
- Refer to privacy, confidentiality and information security in accordance with existing Defence policies and guidelines.
- Address copyright and defamation issues.
- Include a reference to all related Defence policies and guidelines.

Finally, the policy should provide guidelines for escalating cases of the inappropriate use of social media. Personnel, and especially commanding officers and warrant officers, should have the necessary understanding and tools to address issues related to the social media space. Specific briefings for commanding officers on social media engagement for both professional and personal use will be required.

4.3.4 Policy development and implementation

Defence may consider developing and implementing social media policy as outlined above, using the following outline of work:

1. Define the role of social media in Defence.
2. Review and rework current key policy pertaining to social media.
3. Align other related policy.
4. Review and rework Service-specific policy.
5. Communicate the finalised policy to members through a program of education.

To implement the new policy effectively, Defence must focus on providing appropriate educational and training materials to deal with the diversity of attitudes and behaviours towards social media within Defence. Education is critical to change management and the successful adoption of social media in line with Defence policies and values.

4.3.5 Role of social media in Defence

Before embarking on policy review and revision, Defence should clearly define what social media is (and what it is not) in the Defence context, including what constitute social media content, channels and use. Defence should also articulate the role of social media in Defence, and define organisational, professional and personal use of social media. The high-level policy must be platform-flexible, have executive sponsorship, and be culturally appropriate in the Australian governmental and legal context.

4.3.6 Current policy on social media

While this review identified a number of social media guideline documents, it identified only one official policy that spans all Defence services and organisations: *DI(G) ADMIN 08-1 Public comment and dissemination of official information by Defence personnel*, which was issued on 5 October 2007 and last reviewed on 5 October 2010.

While *DI(G) ADMIN 08-1* makes some inroads in governing social media practice in Defence, there are opportunities for clarification. First, while social media are considered within the document as part of ‘new media’, it lacks a clear definition of ‘social media’. There are also some internal inconsistencies in it that may result in misinterpretation and confusion.

Defence should consider reviewing the *DI(G) ADMIN 08-1* policy and creating a new section that outlines how existing policy should be applied in social media contexts. It is important that existing policy covering public comment and official information dissemination is not contradicted by the social media policy.

Once social media has been defined and policy inconsistencies have been resolved, Defence may wish to develop a decision tree type guide to help personnel locate the social media policy section appropriate to their situation (an example is shown in Figure 4.11). A platform-neutral scenario tree will help provide high-level guidance to personnel, without having to have guidelines for every situation that might arise.

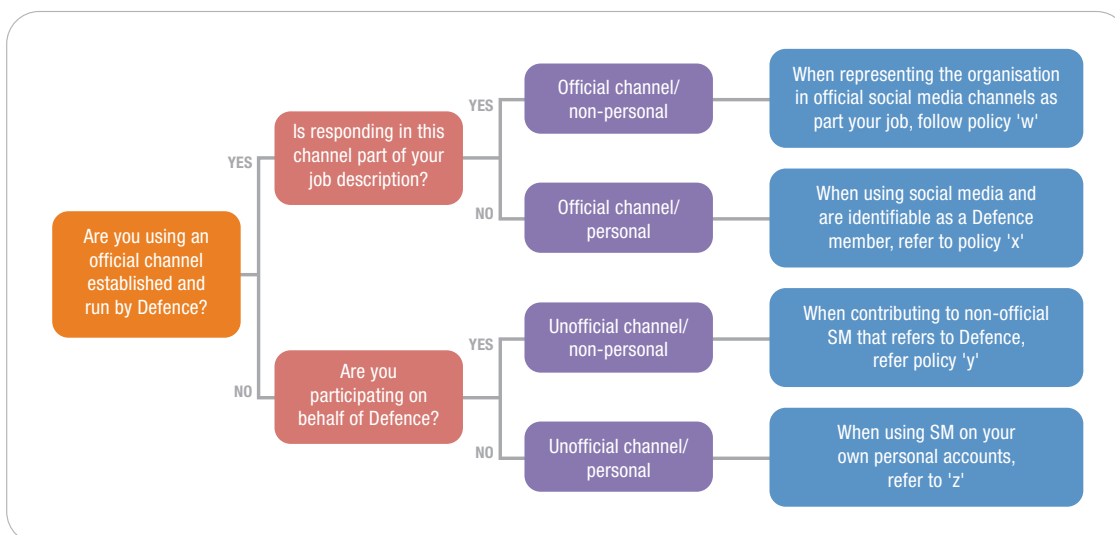


Figure 4.11: A decision tree for social media use

4.3.7 Alignment with other policies

It is important that other references to social media in documents such as the *Protective security policy* are complementary and do not make any conflicting statements. Another specific policy for review is the *DI(G) ADMIN 10-6 Use of Defence telephone and computer resources*. Because of rapid technological advances, *DI(G) ADMIN 106* requires a clearer definition of computer use and personal devices (such as smart phones and PDAs). It should also address the needs of social media teams within Defence who require access to social media sites to conduct Defence business, such as Facebook page administration.

Service-specific policies and organisational policies for organisations such as ADFA should be reviewed and revised. The overarching policy should set the social media direction for all of Defence, and local policy should stipulate how that is executed locally to accommodate unique needs. Again, local policy should be consistent with and not contradict central social media policy, including SOPs.

4.3.8 Standard operating procedures for personnel

SOPs for administrators managing official social media channels

Both the Navy and the Army have already drafted some guidelines and SOPs for administrators of social media channels. That material should be reviewed to ensure that it is consistent with the overall social media policy. Although the Services have slightly different requirements, they should collaborate to ensure broad consistency in guidelines, policies and endorsements by senior command.

Terms of use for official channels

The terms of use should be consistent for all official Defence social media channels. DEOC should review the current terms as published on the individual Service pages and advise on updates as required.

SOPs for Defence personnel who use social media

By clearly defining and communicating acceptable and unacceptable behaviour in social media use, Defence will mitigate its risks. Past problems involving social platforms may have been exacerbated by unclear definitions of appropriate and acceptable behaviour.

The language and tone of the SOPs for all Defence personnel should include everyday and vernacular terms, as in international best practice documents examined in this review and as used in the *US Army social media handbook*. Official needs and OPSEC should be demonstrated through examples and should be conveyed in clear, everyday language.

Defence may wish to reserve the right to ask that certain subjects be avoided and to request members to withdraw certain posts or remove inappropriate comments resulting from private use when the interests of Defence and a member's employment are involved.

Australian Defence Force Academy

ADFA should also consider reviewing its social media rules and educational practices to comply with the broader Defence social media policy. Although there might be some slight differences due to the position of cadets within Defence, establishing proper social media behaviours early will minimise potential career risks at a later date. Given the average age of the recruits and their likely level of internet use and integration into social media activity, it is important to ensure that they understand their obligations and responsibility to behave in an appropriate manner.

4.3.9 Education

Education is fundamental in establishing baseline for social media use across Defence and for effective implementation of the policy. To date, social media education has been sporadic, and has relied on the exercise of 'common sense' and 'professional judgement'. While the organisation may have its own clearly defined view of what it requires, the exercise of discretion requires the subjective interpretation of these terms by individuals, some of whom are relatively young, inexperienced and unable to foresee the damage that may be caused by the inappropriate use of social media. Therefore, Defence should consider reviewing all its social media training packages to align them with the updated policy. The training materials should demonstrate how the central and local policies interlink and should also emphasise the overarching 'ground rules', such as OPSEC and Defence values.

While central social media education should focus on guidelines and principles, locally delivered education should focus on scenarios that personnel in the particular Service might find themselves in because of their local circumstances. For example, an Army cadet may be more vulnerable to social media misuse at home, while a deployed seaman may be more likely to compromise Defence when blogging to family back home. Local education should also address 'common sense' explicitly, to alert personnel to assumptions they might have made based on their own experiences.

Education and training need to be tailored to different stakeholder groups, according to their requirements and level of understanding of social media:

- Executive-level training should focus on education about opportunities and risks associated with social media use and should 'on board' leaders in the organisation.
- Middle managers should be equipped with the skills and knowledge to support and help implement social media practices within their local areas. This can include details such as approval processes for content publishing on the official social media channels and escalation procedures for inappropriate use.
- Personnel should be trained in how to use social media to ensure the responsible representation of Defence, and in how to access relevant policy.

Finally, education should go beyond Defence personnel to include families' social media activities. Family and friends should be provided with support and guidelines to communicate safely with their loved ones using the channels. The guidelines can also be provided to the Defence Community Organisation, *Defence Family Matters* magazine and Defence Families Australia to reinforce the necessity to protect family privacy, OPSEC and security.

4.4 CRISIS MANAGEMENT STRATEGY

To mitigate communication risks in social media effectively, it is necessary for Defence to define clearly what type of content is concerning or undesirable. Various content could cause concern, but Defence should be able to set out a scale for prioritising responses that balances the severity and the probability of particular types of postings. Once a scale is available, escalation procedures can be carried out to respond in a timely and accurate manner. To be considered a crisis, the communication of undesirable information will be very rapid, very wide, or both.

Not all undesirable content will produce crises, so a triage system for assessing problem content as it comes to hand should be implemented. This will ensure that problems are mitigated appropriately, according to the probability that they will produce a crisis and the severity of resulting damage. The aim is to prevent crises occurring by identifying and dealing with problems early, where possible. Should a crisis escalate, Defence should be prepared to address it according to the crisis management protocol.

PR teams are best equipped to generate reactive communication to protect the brands and reputation of Defence. However, negative mentions in traditional media do not necessarily drive negative social media conversation. Often, negative mentions can encourage positive conversations, as advocates in social media defend the brand against the traditional media's positioning of the issue. Before responding to negative sentiment or postings, it is necessary to identify the type of problem as well as its severity.

Social media crises can include the following types:

- OPSEC breaches
- personal security or privacy breaches
- Marketing/PR – originated offline – propagated online
- Marketing/PR – originated online – propagated online
- Marketing/PR – originated online – propagated offline.

Identifying the source and type of breach helps to define the most appropriate response. While this review was given the task of examining the management of employee-generated crises, problems in social media can originate from a variety of other sources,

such as the media, online communities and the general public.

The management of a crisis that originates in social media but is propagated offline (usually by mainstream media) should follow Defence's existing procedures for media management, with the addition of maintaining a vigil in the social space. However, Defence's 'offline' procedures are mostly understood by a few public affairs specialists, so high-level documentation would be beneficial in defining online processes. The remaining types of social media crisis should be handled online. Suggested actions to be taken in response to a social media crisis are set out in Table 4.5.

Type	Action
OPSEC Breach > online	<ul style="list-style-type: none"> • Remove offending content (or request its removal). • Contact individual responsible for breach and educate them about their actions in the first instance. • If the individual continues the breach, disciplinary action should be taken in accordance with Defence disciplinary protocol. • Monitor for rumours or rebroadcasting of material and, where possible, replace rumours with facts.
Marketing/PR offline > online	<ul style="list-style-type: none"> • Respond to all channels with a consistent message • Monitor for rumours or rebroadcasting of materials and where possible replace rumours with facts.
Marketing/PR online > online	<ul style="list-style-type: none"> • Respond online only (no need to deepen or spread the crisis) • Monitor for rumours or rebroadcasting of materials and where possible replace rumours with facts.
Marketing/PR online > offline	<ul style="list-style-type: none"> • Apply existing offline crisis management processes.

Table 4.5: Examples of organisational responses to a social media crisis

Facebook provides crisis management guidelines for commercial businesses using social media. Some of the guidelines, such as identifying the problem and determining the validity of the source, clearly apply to Defence (Figure 4.12). Other points, such as 'Empower your loyal consumers and advocates' can apply to family members in Defence's 'safe spaces' in social media. Defence community members should not be expected to shield Defence or its brands, but some will inevitably attempt to do so, motivated by loyalty and pride. This is another reason why Defence should consider a wider education program for social media use that goes beyond its own personnel.

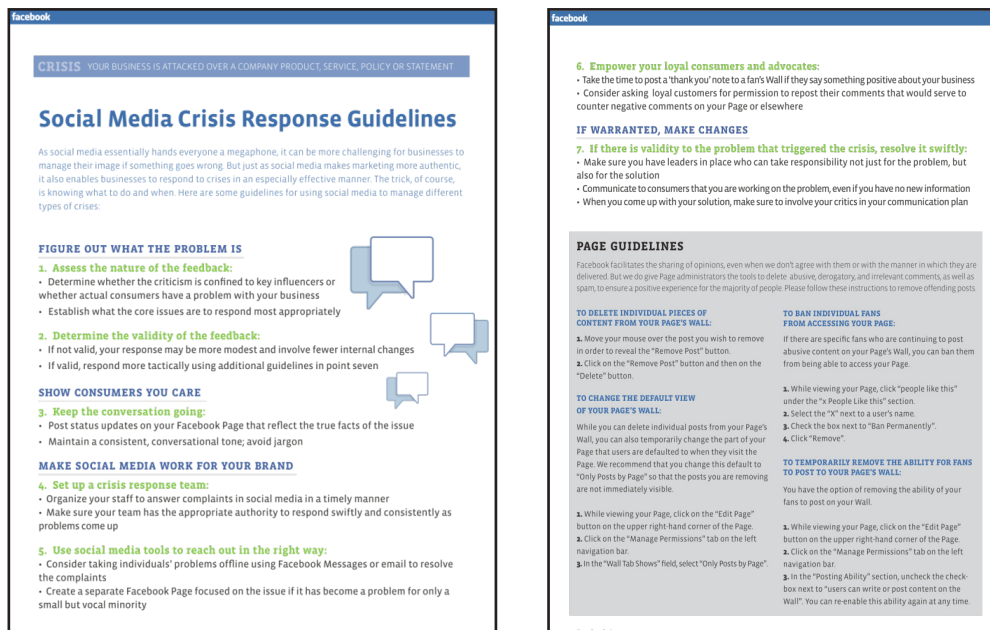


Figure 4.12: Facebook social media crisis response guidelines

(Source: http://ads.ak.facebook.com/ads/FacebookAds/SocialMediaCrisisGuidelines_041911.pdf, retrieved 27 July 2011)

Crisis management, PR, marketing and branding are all interconnected, which implies that a crisis plan cannot be developed without the involvement of stakeholders from all of those fields, in addition to Intelligence services. The 'crawl, walk, run and fly' business strategy, as outlined in Section 4.1 of this report, works as a strategy for Defence in social media. The 'fly' phase is actioned only when a crisis is occurring and should be developed as an important part of the overall strategy. Crisis management is generally reactive, but can be developed proactively with a marketing and communications plan to provide communications staff with guidelines on how to react.

The key steps in the crisis management plan are to identify the crisis, plan the response in line with the guidelines, respond to the crisis, and monitor the response (Figure 4.55). Those steps continue until a crisis is no longer identified in Phase 1. Crises or potential crises can often be identified through regular monitoring and careful moderating of social media spaces using a combination of software and human analysis.

4.4.1 Crisis identification

The following questions should be asked to assess whether a negative situation might be considered a crisis and how a response should be developed:

- What is the type of issue?
- Is the issue in more than one channel?
- Can the issue be managed through existing offline crisis management methods?
- Will a response aggravate or mitigate the crisis?
- Are there legal considerations to the response?
- Who is the best person to address the crisis?
- Are offline media likely to quote responses or escalate the situation via traditional channels?

Communications staff responsible for managing social media should be given the training to respond to negative situations quickly and flexibly. Social media are a few of many channels where communication occurs, and many journalists use them to investigate or source stories. Therefore, public relations in the social media should be given the same consideration as broadcast media public relations.

Not all Defence members need to use social media to communicate officially with the general public, just as they are not all permitted to talk officially to the traditional media. Official communication should be restricted to those who are experienced at communicating the message of Defence in other channels, but with specific crisis management training in social media and other digital channels. Approval processes for communication in a crisis should be fast-tracked so that core values are upheld, without delays in responses that could create a knowledge void (described below) and further damage to Defence.

4.4.2 Tips for communications staff in responding to a social media crisis

- Stay in your lane (respond only to issues within your area of expertise or that you have consulted knowledge owners about).
- Consult a social media adviser before taking action.
- Take a breath. Fill space carefully, not emotionally.
- Consider whether your response will inflame the crisis or create a new one.
- Delete and/or report OPSEC breaches immediately, and inform the social media adviser and the individual responsible for the breach.

While communications staff should receive special training and resources to respond to social media crises, other personnel will also require guidance on reporting and escalating concerning content they see in social media channels.

4.4.3 Emergency response monitoring

In addition to day-to-day monitoring, emergency monitoring can be set up in a crisis. It can include a combination of feeds and alerts designed to give an instant snapshot of conversations happening online. Standard monitoring tools often take 24 hours to process data, which can be too slow in a crisis. Emergency monitoring should bring together a combination of near realtime tools and continuous human monitoring of all conversations for the duration of the crisis. Responses to that information can then be made instantly or fed to the communications team for further advice.

4.4.4 The 'knowledge void'

A knowledge void is an inactive period during communication that creates an opportunity for rumours to start and unofficial presences to expand and grow. For example, when a negative comment is posted about Defence, the lag time between the initial comment and a response from Defence creates a knowledge void.

To counter this possibility, Defence should aim to be the trusted source of information for the audience. Consistent branding is one way audiences identify information as 'official', which is why it is important for the Services to have a well-managed and well-populated presence in social media before a crisis arises. This ensures that community members will know where to get factual information directly from the source, allowing them to share it with their networks and thereby aid the crisis management effort. In addition, if a response must be delayed, the issue should at least be acknowledged and the expected response time provided in order to manage expectations.

This review discusses crisis management in Defence-owned social media channels, but ignoring content in unofficial channels can also produce a crisis. If no official information is available, unofficial channels have an opportunity to communicate their own 'information' or agenda, which can then be shared by others in their networks. This action can have the opposite effect of crisis management and can create a new crisis through the spreading of rumours or untruths, often unintentionally. Communities want information about issues that affect them, and gaps in knowledge will often be filled by someone with a receptive audience ready to believe unofficial and potentially incorrect information.

If you don't become the trusted source for information, someone else will.

4.4.5 Crisis exit strategy

In early trials of social media within Defence, several pages were created that were later abandoned due to lack of results or resources. It is important that these and similar future pages are not simply left in cyberspace without any information about why they are no longer active, while at the same time acting as an alternative source of information. For example, this review found a locked Defence Twitter account with no explanation about why the account was locked. This creates the impression that Defence is publishing material that it does not want open to the public. While that is not true, the effect on the brand could be negative and the action could generate rumours and false information.

Most such trials are conducted in 'safe spaces', and there is nothing wrong with informing the audience that a social media presence is a trial or in beta. It is often beneficial to engage the audience in the trial and make them feel part of the process by allowing them to provide feedback. This has the added advantage that questioning users about their experience in order to improve the site does not raise suspicions. It also means that problems with the page can be raised with the audience, which usually produces positive support from users.

If the goal of the social media presence has not been met or a lack of resources makes it impossible to continue, that should be communicated to the audience. This can be done by publishing a post stating why the page or presence is no longer active, with a link or direction on where to go for further information or to contact the owners. In the case of Facebook, skyscraper profile pictures can be used to communicate the movement or closing down of the page. However, once the message is communicated, a dead space should not be left in social media.

ANNEX 1

QUALITATIVE AND QUANTITATIVE RESEARCH

ANNEX 1 QUALITATIVE AND QUANTITATIVE RESEARCH

This review undertook qualitative and quantitative research to better understand Defence members' social media activities and beliefs about social media.

The qualitative research consisted of more than 26 hours of one-to-one interviews with stakeholders across Defence, including 31 cadets at ADFA. The results have been considered throughout the review and have been reflected in the findings in this report.

Quantitative research was undertaken with 1,577 members of Defence, and with an additional 1,000 members of the general public, in order to draw comparisons between the two groups.

The public responses required no weighting, due to the survey's use of quota control. Defence responses required some minor weighting of age, gender and rank demographic, in order to address slight response skewing. The weighting was calculated using April 2010 employment statistics, derived from PMKeyS data supplied by Defence.

All quantitative research was undertaken via an online questionnaire, after potential respondents were informed by email of their random selection from predefined demographic groups based on current rank or employment level.

Taking into account population and numbers of respondents, responses were collated into three groups: the public; the Department of Defence; and the Navy, Army and Air Force. The resulting 15 reporting groups were used to formulate the findings in this annex. An additional group of non-employed general public (D) was also defined to fairly represent that demographic. A breakdown of roles and levels within each reporting group is shown below. These categorisations are in line with the standard reporting methods provided by the Director of Strategic Personnel Policy Research.

Army, Navy and RAAF		Department of Defence	Public
A	CMDR/LTCOL/WGCDR CAPT/COL/GPCAPT CDRE/BRIG/AIRCDRE RADM/MAJGEN/AVM	SES Band 1 & above	Academic Consultant Senior Manager / Director
	MIDN/OCDT/SCDT/OFF CADET ASLT/2 LT/PLTOFF SBLT/LT/FLGOFF LEUT/CAPT/FLTLT LCDR/MAJ/SQNLDR	Executive Level 1 or equivalent Executive Level 2 or equivalent S&T Level 5 S&T Level 6 S&T Level 7 S&T Level 8	Manager Business Owner Associate Professional
	PO/SGT SSGT CPO/WO2/FSGT WO/WO1/WOFF	APS Level 5 or equivalent APS Level 6 or equivalent S&T Level 3 S&T Level 4	Professional Design / Creative
	Recruit SMN/PTE(E)/AC/ACW AB/LCPL/LAC/LACW LS/CPL/CPL(E)	Trainee APS APS Level 1 or equivalent APS Level 2 or equivalent APS Level 3 or equivalent APS Level 4 or equivalent S&T Level 1 S&T Level 2	Administrator Tradesperson Clerical, Sales, or Service worker Production or Transport worker Labourer Voluntary work Student
D	Reserved for whole of population reporting (n=86)		Unemployed Home duties Retired

The resulting respondents, levels where shown below.

	Army	Navy	RAAF	DoD	Public
Job / Rank / Level A	127	104	116	115	286
Job / Rank / Level B	92	71	64	191	187
Job / Rank / Level C	264	161	149	123	441
Job / Level D					86
TOTAL	483	336	329	429	1000

The online survey and sourcing of public respondents was carried out by Edentify Pty Ltd, which describes its methodology as follows:

Edentify owns and operates a dedicated online research panel – www.cafestudy.com – with over 35,000 active members. Consumers are recruited to join the panel through ongoing targeted advertising around an overall strategy of building a representative and robust consumer database Australia wide. Advertising consists predominantly of banner ads on carefully selected websites alongside offline marketing in the form of print ads and postcards. Edentify uses this panel to source the target audience for quantitative projects (online surveys and mobile polling) and qualitative projects (online forums).

In return for taking part in research studies participants are rewarded for their time and efforts through a point based system – this ensures participation rates are maintained.

All quantitative research undertaken by this review was conducted between 5 and 12 July 2011 and all respondents were anonymous. The fact that respondents would be anonymous was communicated to them before the survey began.

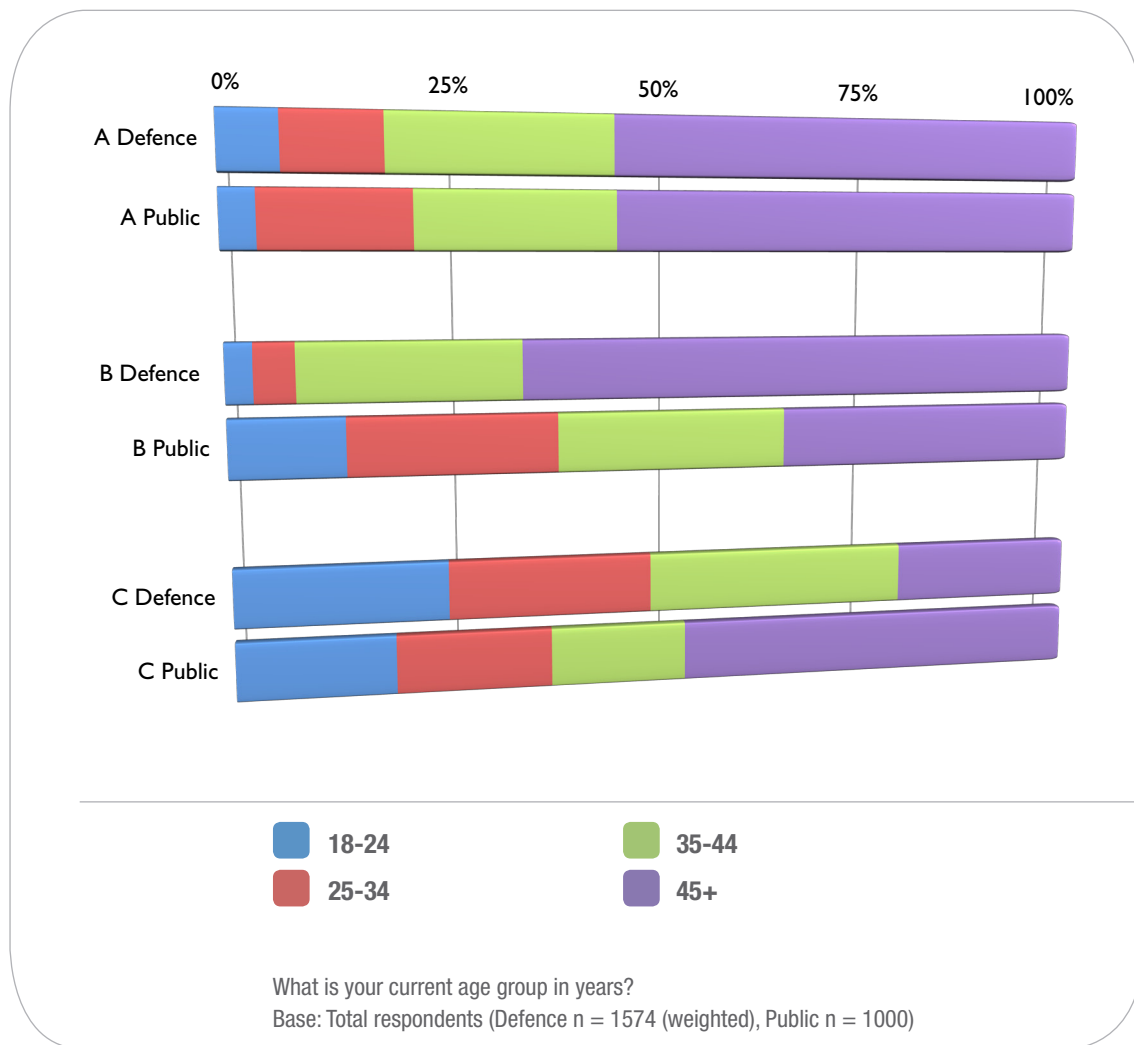
Data presented in this section shows differing usage of social media by personnel within Defence organisations. The differences do not necessarily reflect respondents' desires or ability. Usage is affected by the availability of internet access to the respondents in their day to day activities. Members who are deployed and those who are not deployed also have differing opportunities to use the web, based on available bandwidth and hardware, and that should be considered when comparing the usage levels of the services.

Please note, the confidence score for the quantitative research is as follows:

Defence : 97.5% (+/- 2.5%)

General population : 97% (+/- 3.1%)

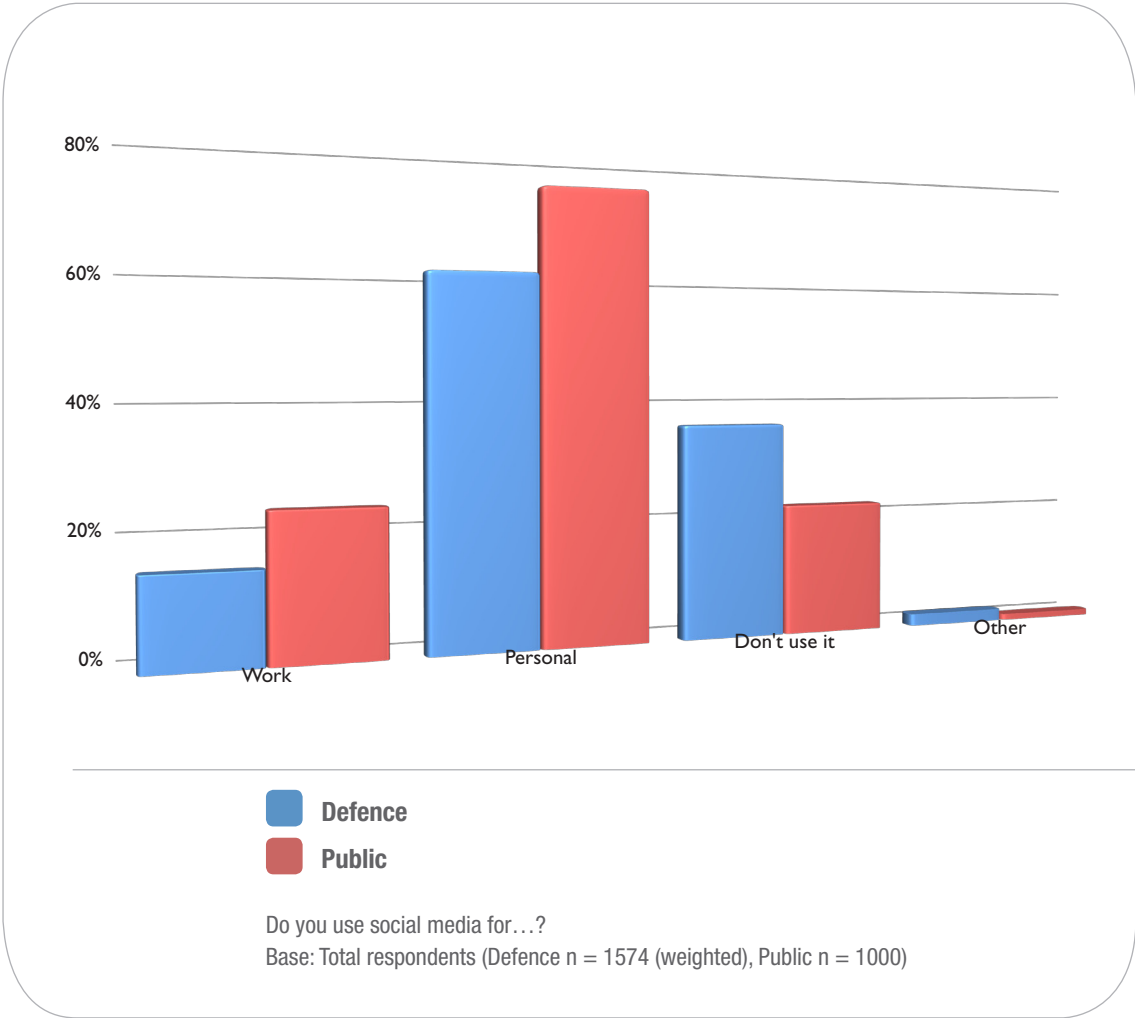
WHAT IS YOUR CURRENT AGE GROUP IN YEARS?



	A Defence	A Public	B Defence	B Public	C Defence	C Public
18-24	7%	4%	3%	13%	24%	18%
25-34	11%	17%	5%	24%	23%	18%
35-44	26%	23%	25%	27%	31%	16%
45+	56%	56%	67%	36%	21%	48%

The age demographic of senior Defence personnel is very similar to that of their public equivalents; both consist of 56% over the age of 45. Defence has an older population in middle management overseeing a younger workforce.

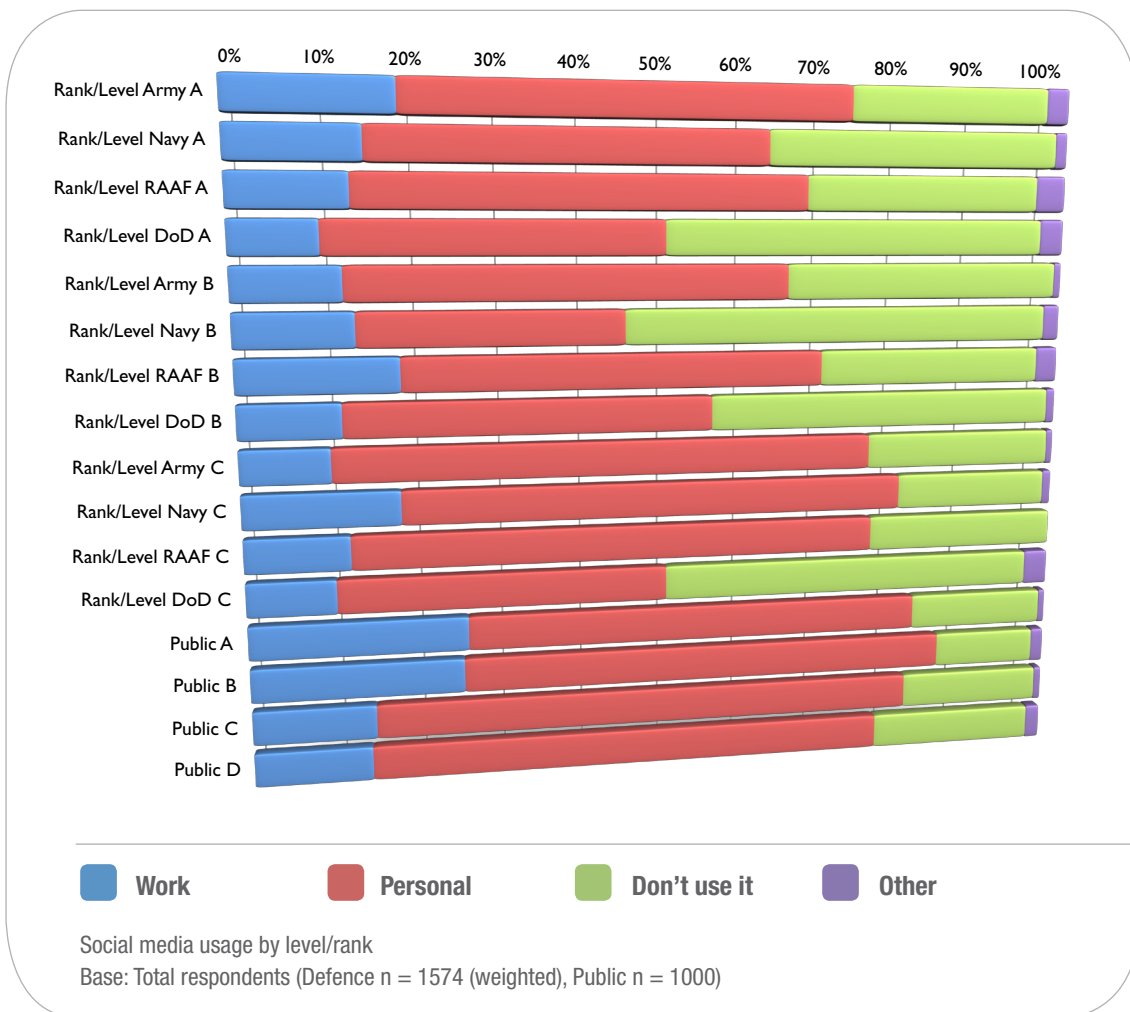
DO YOU USE SOCIAL MEDIA FOR...?



	Defence	Public
Work	15%	24%
Personal	61%	75%
Other	2%	1%
Don't use it	36%	22%

The Australian public has a far greater propensity to use social media than those employed in Defence. Only 22% of Australians claim *not* to use social media, compared to over a third of Defence employees.

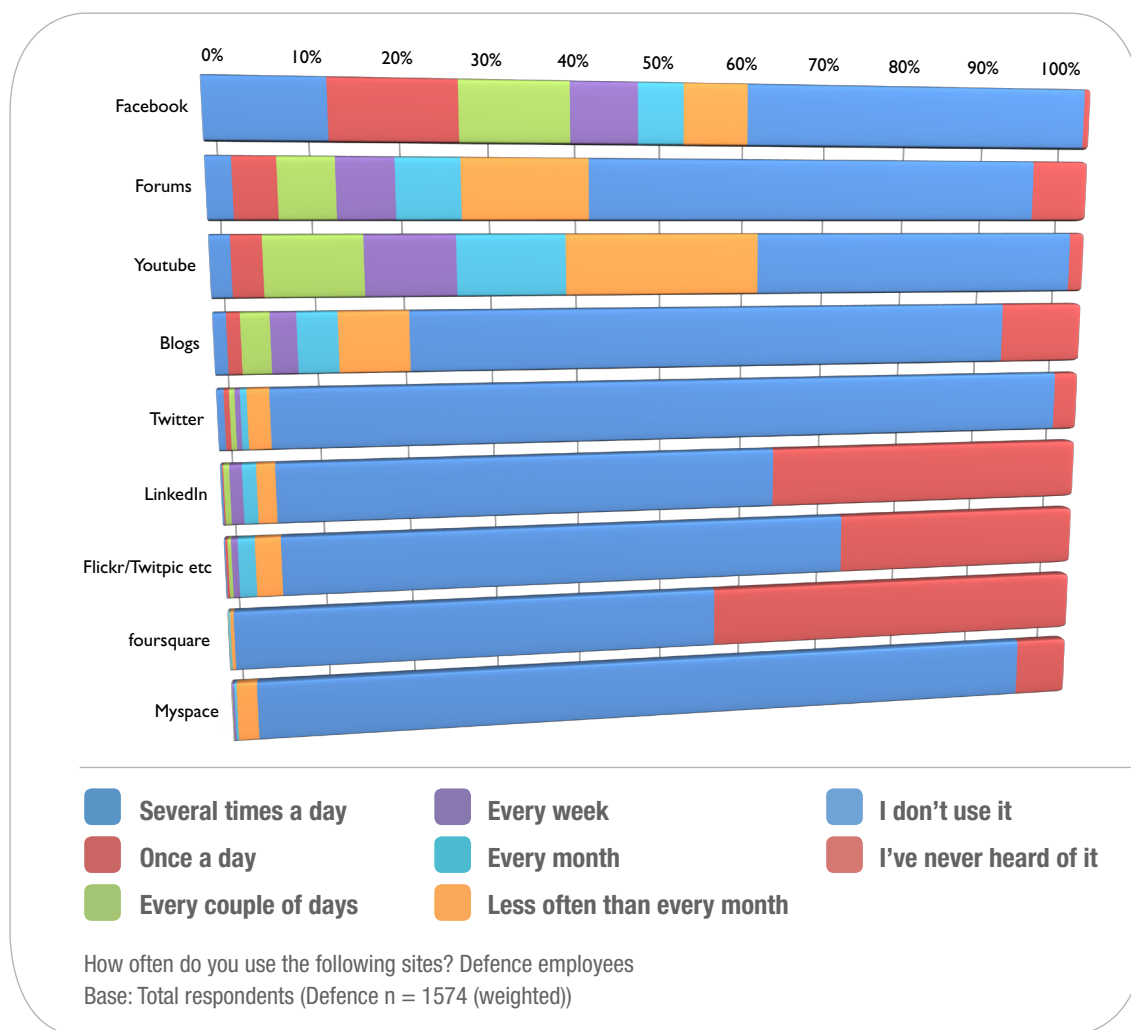
SOCIAL MEDIA USAGE BY LEVEL/RANK



	Defence Total	Army A	Navy A	RAAF A	DoD A	Army B	Navy B	RAAF B	DoD B	Army C	Navy C	RAAF C	DoD C	Public Total	Public A	Public B	Public C	Public D
Work	15%	23%	18%	16%	11%	14%	15%	23%	13%	11%	22%	14%	11%	24%	33%	33%	17%	16%
Personal	61%	64%	56%	63%	44%	58%	35%	61%	49%	72%	74%	72%	43%	75%	72%	79%	78%	73%
Don't use it	36%	30%	43%	34%	52%	38%	59%	34%	48%	26%	23%	27%	51%	22%	22%	17%	21%	24%
Other	2%	3%	2%	4%	3%	1%	2%	3%	1%	1%	1%	0%	3%	1%	1%	2%	1%	2%

Generally speaking, those employed in Defence Level/Rank C are far more likely to use social media than those at Level/Rank A or B. In fact, their usage is at much the same level as the general public's, the exception being DoD Level/Rank C, of whom less than half claim to use it at all. This is likely due to the fact that those employed in this group are older than their Army/Navy/RAAF counterparts.

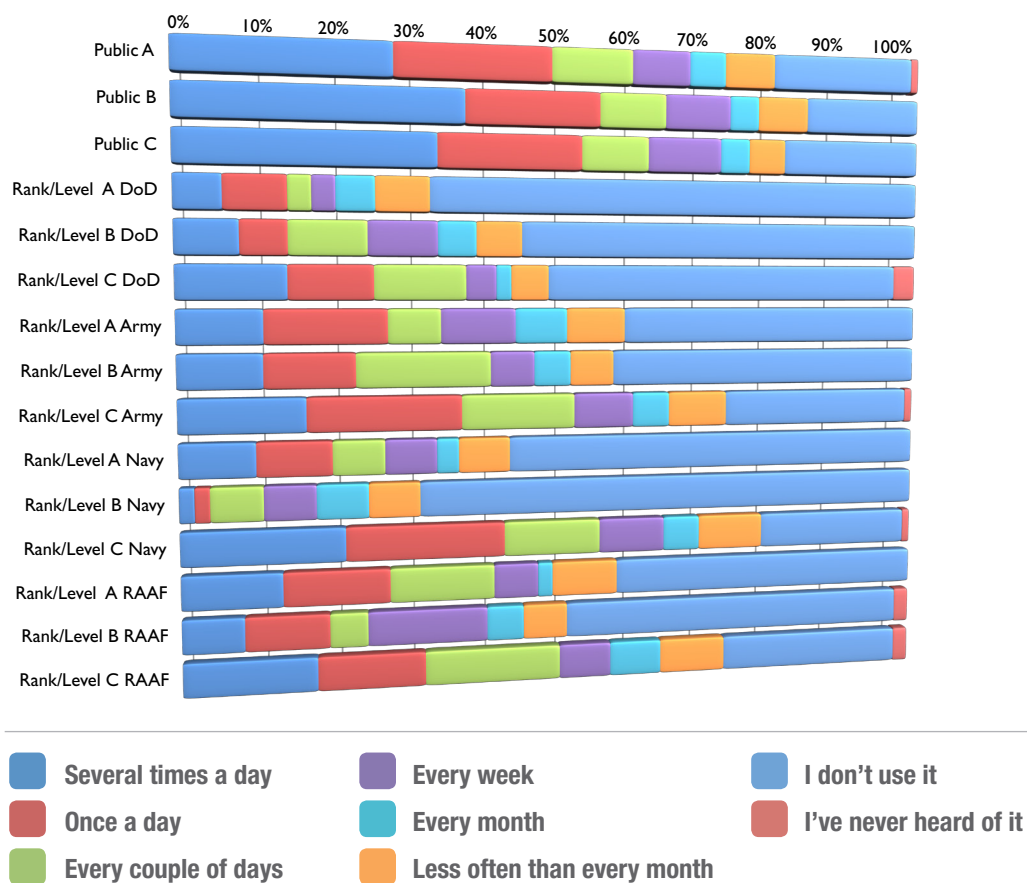
HOW OFTEN DO YOU USE THE FOLLOWING SITES? DEFENCE EMPLOYEES



	Several times a day	Once a day	Every couple of days	Every week	Every month	Less often than every month	I don't use it	I've never heard of it
Myspace	0%	0%	0%	0%	0%	2%	91%	6%
foursquare	0%	0%	0%	0%	0%	0%	55%	45%
Flickr/Twitpic etc	0%	0%	0%	1%	2%	3%	65%	29%
LinkedIn	0%	0%	1%	1%	2%	2%	56%	38%
Twitter	1%	1%	1%	1%	1%	2%	92%	3%
Blogs	1%	1%	3%	3%	4%	8%	69%	10%
YouTube	2%	3%	11%	10%	12%	22%	38%	2%
Forums	3%	5%	6%	6%	7%	14%	52%	7%
Facebook	13%	14%	12%	8%	5%	7%	40%	1%

Facebook is by far the most popular social media site, with around one in four Defence employees indicating that they use it every day. Forums and YouTube also see a reasonably high level of usage, although less frequent. At the other end of the scale, very few people are using foursquare or Myspace, with of foursquare is particularly low.

FACEBOOK USE



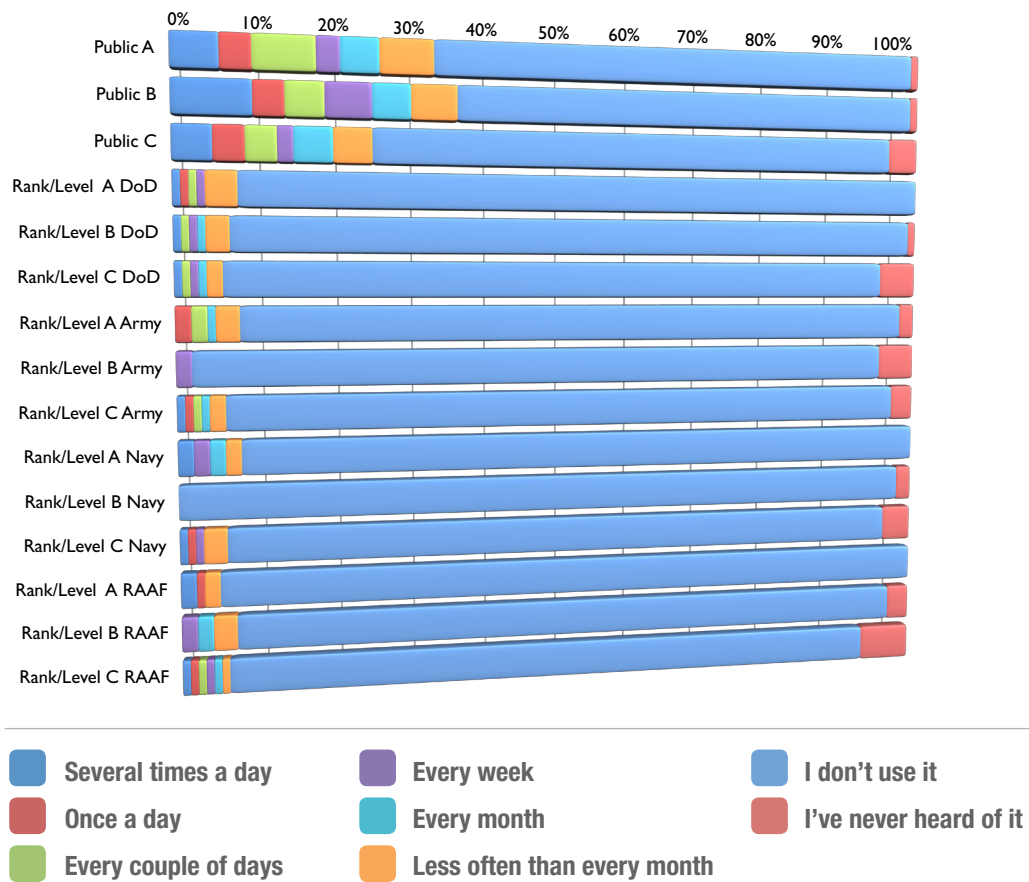
About how often would you say you use the following social media sites?

Base: Total respondents (Defence n = 1574 (weighted), Public n = 1000)

	Several times a day	Once a day	Every couple of days	Every week	Every month	Less often than every month	I don't use it	I've never heard of it
Public A	28%	21%	11%	8%	5%	7%	20%	1%
Public B	37%	18%	9%	9%	4%	7%	16%	0%
Public C	33%	19%	9%	10%	4%	5%	19%	0%
Rank/Level A DoD	6%	8%	3%	3%	5%	7%	67%	0%
Rank/Level B DoD	8%	6%	10%	9%	5%	6%	55%	0%
Rank/Level C DoD	14%	11%	12%	4%	2%	5%	49%	3%
Rank/Level A Army	11%	16%	7%	10%	7%	8%	42%	0%
Rank/Level B Army	11%	12%	18%	6%	5%	6%	44%	0%
Rank/Level C Army	16%	20%	15%	8%	5%	8%	26%	1%
Rank/Level A Navy	10%	10%	7%	7%	3%	7%	59%	0%
Rank/Level B Navy	2%	2%	7%	7%	7%	7%	72%	0%
Rank/Level C Navy	21%	21%	13%	9%	5%	9%	21%	1%
Rank/Level A RAAF	13%	14%	14%	6%	2%	9%	43%	0%
Rank/Level B RAAF	8%	11%	5%	16%	5%	6%	48%	2%
Rank/Level C RAAF	17%	14%	18%	7%	7%	9%	25%	2%

Within Defence, Facebook is used the most by Rank/Level C. The lowest users are Rank/Level Bs in Army, Navy and RAAF. Among the public Public B are the highest users, albeit by a small margin.

TWITTER USE

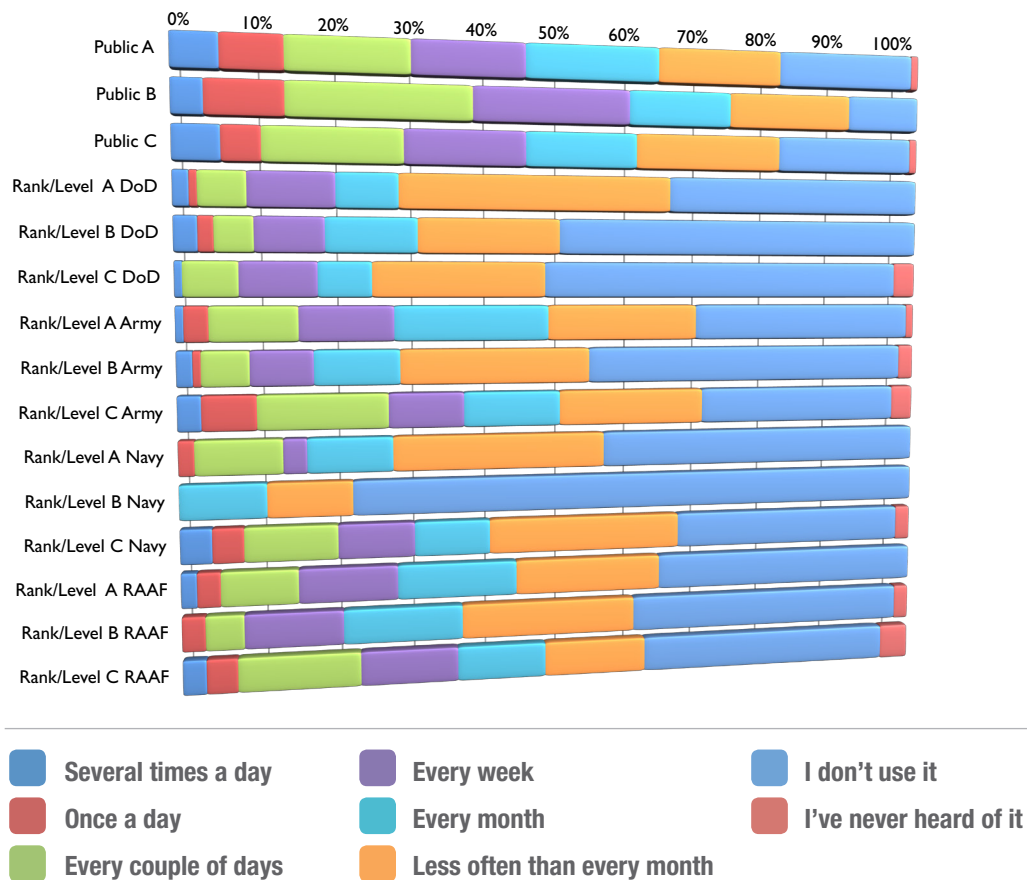


About how often would you say you use the following social media sites?
Base: Total respondents (Defence n = 1574 (weighted), Public n = 1000)

	Several times a day	Once a day	Every couple of days	Every week	Every month	Less often than every month	I don't use it	I've never heard of it
Public A	6%	4%	8%	3%	5%	7%	66%	1%
Public B	10%	4%	5%	6%	5%	6%	63%	1%
Public C	5%	4%	4%	2%	5%	5%	71%	4%
Rank/Level A DoD	1%	1%	1%	1%	0%	4%	92%	0%
Rank/Level B DoD	1%	0%	1%	1%	1%	3%	93%	1%
Rank/Level C DoD	1%	0%	1%	1%	1%	2%	89%	5%
Rank/Level A Army	0%	2%	2%	0%	1%	3%	90%	2%
Rank/Level B Army	0%	0%	0%	2%	0%	0%	94%	5%
Rank/Level C Army	1%	1%	1%	0%	1%	2%	90%	3%
Rank/Level A Navy	2%	0%	0%	2%	2%	2%	93%	0%
Rank/Level B Navy	0%	0%	0%	0%	0%	0%	98%	2%
Rank/Level C Navy	1%	1%	0%	1%	0%	3%	91%	4%
Rank/Level A RAAF	2%	1%	0%	0%	0%	2%	96%	0%
Rank/Level B RAAF	0%	0%	0%	2%	2%	3%	90%	3%
Rank/Level C RAAF	1%	1%	1%	1%	1%	1%	88%	7%

Across the board, awareness of Twitter is high; however, this is only reflected in the volume of use by the public. The highest users of Twitter within Defence are Rank/Level A.

YOUTUBE USE

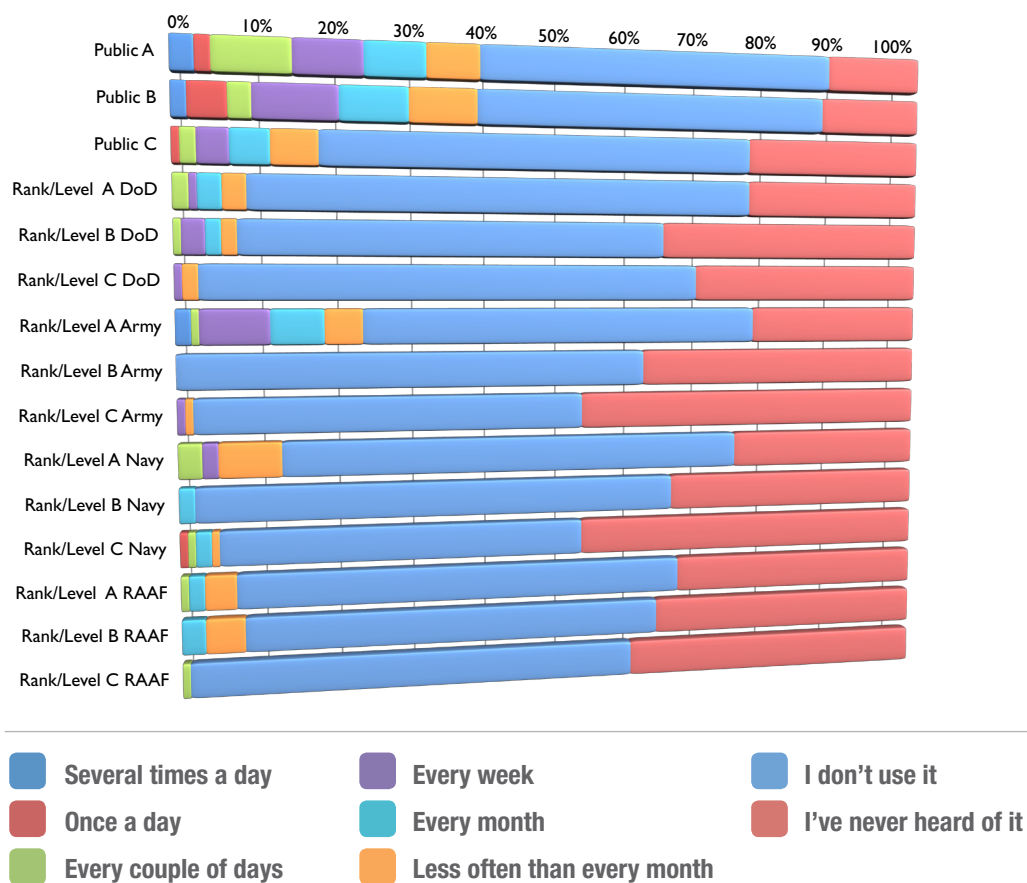


About how often would you say you use the following social media sites?
 Base: Total respondents (Defence n = 1574 (weighted), Public n = 1000)

	Several times a day	Once a day	Every couple of days	Every week	Every month	Less often than every month	I don't use it	I've never heard of it
Public A	6%	8%	16%	15%	18%	17%	19%	1%
Public B	4%	10%	24%	21%	14%	17%	10%	0%
Public C	6%	5%	18%	16%	15%	20%	19%	1%
Rank/Level A DoD	2%	1%	6%	11%	8%	36%	35%	0%
Rank/Level B DoD	3%	2%	5%	9%	12%	19%	51%	0%
Rank/Level C DoD	1%	0%	7%	10%	7%	23%	50%	3%
Rank/Level A Army	1%	3%	11%	12%	20%	20%	30%	1%
Rank/Level B Army	2%	1%	6%	8%	11%	25%	44%	2%
Rank/Level C Army	3%	7%	17%	10%	13%	20%	28%	3%
Rank/Level A Navy	0%	2%	11%	3%	11%	28%	44%	0%
Rank/Level B Navy	0%	0%	0%	0%	11%	11%	78%	0%
Rank/Level C Navy	4%	4%	12%	10%	10%	26%	32%	2%
Rank/Level A RAAF	2%	3%	10%	13%	16%	20%	37%	0%
Rank/Level B RAAF	0%	3%	5%	13%	16%	24%	39%	2%
Rank/Level C RAAF	3%	4%	16%	13%	12%	14%	35%	4%

Awareness of YouTube is high for all segments but its use is less frequent within Defence. Rank/Level B Navy are the lowest users by a wide margin, with no users more frequent than monthly.

LINKEDIN USE



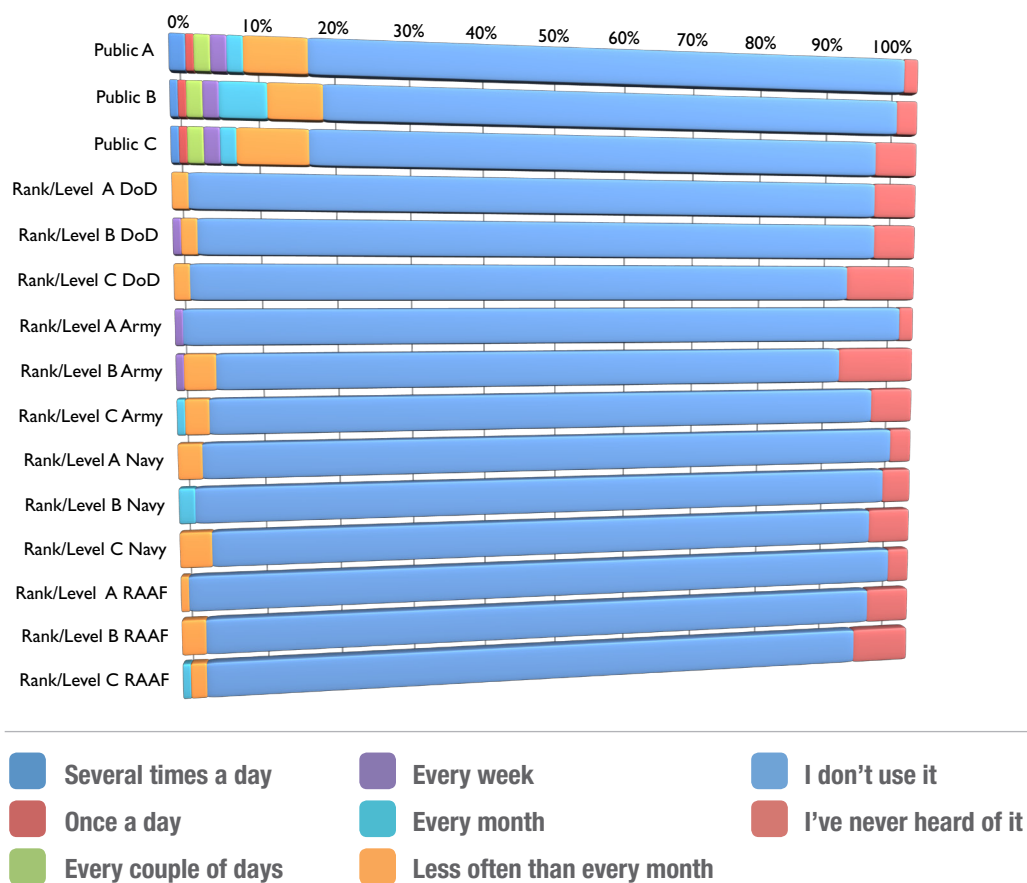
About how often would you say you use the following social media sites?

Base: Total respondents (Defence n = 1574 (weighted), Public n = 1000)

	Several times a day	Once a day	Every couple of days	Every week	Every month	Less often than every month	I don't use it	I've never heard of it
Public A	3%	2%	10%	9%	8%	7%	48%	13%
Public B	2%	5%	3%	11%	9%	9%	48%	14%
Public C	0%	1%	2%	4%	5%	6%	57%	24%
Rank/Level A DoD	0%	0%	2%	1%	3%	3%	66%	24%
Rank/Level B DoD	0%	0%	1%	3%	2%	2%	57%	37%
Rank/Level C DoD	0%	0%	0%	1%	0%	2%	66%	32%
Rank/Level A Army	2%	0%	1%	9%	7%	5%	54%	24%
Rank/Level B Army	0%	0%	0%	0%	0%	0%	61%	39%
Rank/Level C Army	0%	0%	0%	1%	0%	1%	50%	47%
Rank/Level A Navy	0%	0%	3%	2%	0%	8%	61%	26%
Rank/Level B Navy	0%	0%	0%	0%	2%	0%	63%	35%
Rank/Level C Navy	0%	1%	1%	0%	2%	1%	48%	48%
Rank/Level A RAAF	0%	0%	1%	0%	2%	4%	59%	34%
Rank/Level B RAAF	0%	0%	0%	0%	3%	5%	55%	37%
Rank/Level C RAAF	0%	0%	1%	0%	0%	0%	59%	41%

Within Defence, awareness of LinkedIn is moderately low; with high use is reflected in the public responses (Level A being the highest users). There are no users of LinkedIn with in Rank/Level B Army.

MYSPACE USE



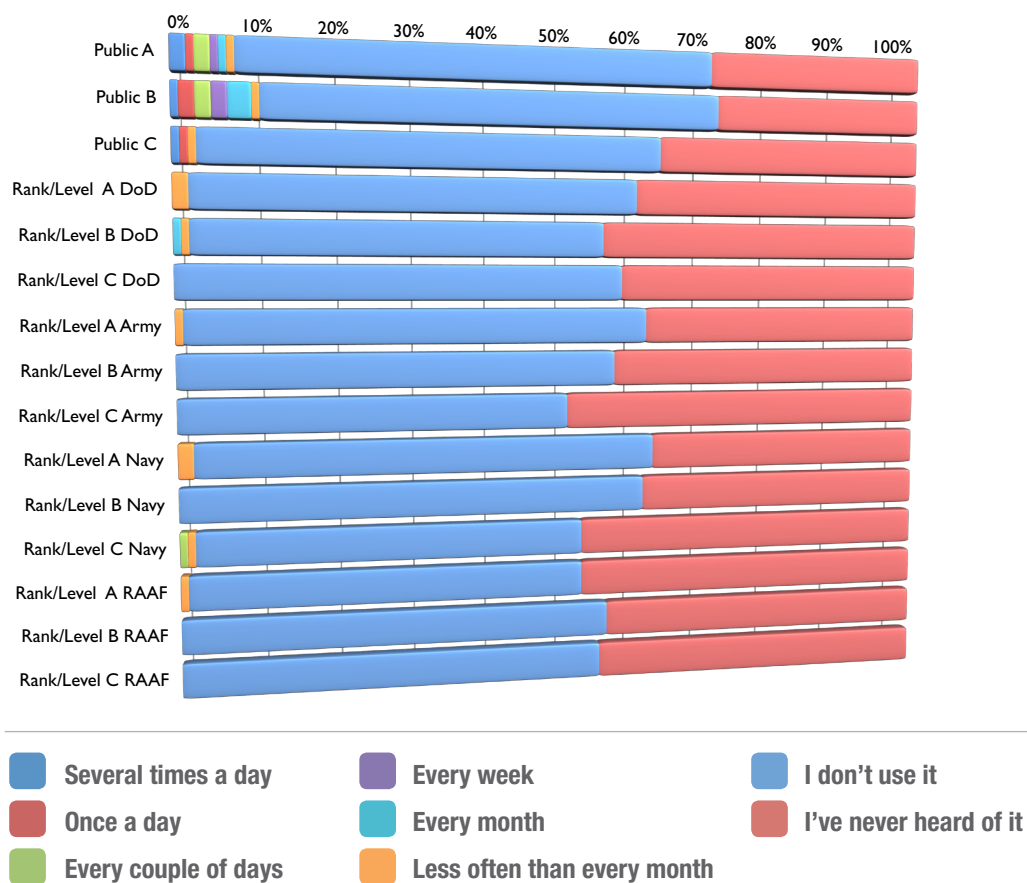
About how often would you say you use the following social media sites?

Base: Total respondents (Defence n = 1574 (weighted), Public n = 1000)

	Several times a day	Once a day	Every couple of days	Every week	Every month	Less often than every month	I don't use it	I've never heard of it
Public A	2%	1%	2%	2%	2%	8%	81%	2%
Public B	1%	1%	2%	2%	6%	7%	79%	3%
Public C	1%	1%	2%	2%	2%	9%	77%	6%
Rank/Level A DoD	0%	0%	0%	0%	0%	2%	91%	6%
Rank/Level B DoD	0%	0%	0%	1%	0%	2%	91%	6%
Rank/Level C DoD	0%	0%	0%	0%	0%	2%	89%	10%
Rank/Level A Army	0%	0%	0%	1%	0%	0%	97%	2%
Rank/Level B Army	0%	0%	0%	1%	0%	4%	85%	11%
Rank/Level C Army	0%	0%	0%	0%	1%	3%	90%	6%
Rank/Level A Navy	0%	0%	0%	0%	0%	3%	93%	3%
Rank/Level B Navy	0%	0%	0%	0%	2%	0%	93%	4%
Rank/Level C Navy	0%	0%	0%	0%	0%	4%	90%	6%
Rank/Level A RAAF	0%	0%	0%	0%	0%	1%	96%	3%
Rank/Level B RAAF	0%	0%	0%	0%	0%	3%	90%	6%
Rank/Level C RAAF	0%	0%	0%	0%	1%	2%	89%	8%

Myspace is well known and rarely used, with only 22% of all respondents and 3% within Defence visiting the site more than monthly.

FOURSQUARE USE

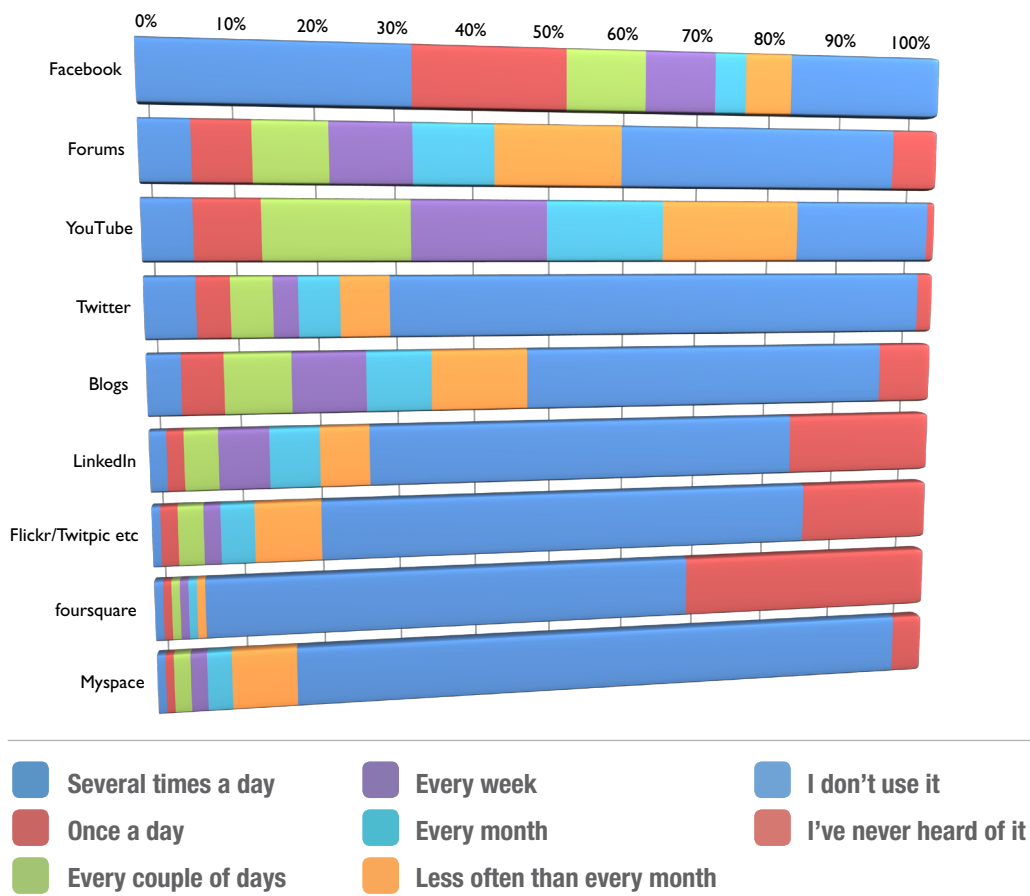


About how often would you say you use the following social media sites?
Base: Total respondents (Defence n = 1574 (weighted), Public n = 1000)

	Several times a day	Once a day	Every couple of days	Every week	Every month	Less often than every month	I don't use it	I've never heard of it
Public A	2%	1%	2%	1%	1%	1%	63%	30%
Public B	1%	2%	2%	2%	3%	1%	61%	29%
Public C	1%	1%	0%	0%	0%	1%	59%	36%
Rank/Level A DoD	0%	0%	0%	0%	0%	2%	58%	40%
Rank/Level B DoD	0%	0%	0%	0%	1%	1%	54%	45%
Rank/Level C DoD	0%	0%	0%	0%	0%	0%	58%	42%
Rank/Level A Army	0%	0%	0%	0%	0%	1%	61%	39%
Rank/Level B Army	0%	0%	0%	0%	0%	0%	57%	43%
Rank/Level C Army	0%	0%	0%	0%	0%	0%	50%	49%
Rank/Level A Navy	0%	0%	0%	0%	0%	2%	61%	38%
Rank/Level B Navy	0%	0%	0%	0%	0%	0%	61%	39%
Rank/Level C Navy	0%	0%	1%	0%	0%	1%	51%	48%
Rank/Level A RAAF	0%	0%	0%	0%	0%	1%	52%	48%
Rank/Level B RAAF	0%	0%	0%	0%	0%	0%	56%	44%
Rank/Level C RAAF	0%	0%	0%	0%	0%	0%	55%	45%

Foursquare has a consistently low awareness and use, the highest users being Public B with only 11% usage. Within Defence, only Rank/Level C Navy use foursquare more frequently than every month, with 1% using foursquare every couple of days.

HOW OFTEN DO YOU USE THE FOLLOWING SITES? AUSTRALIAN PUBLIC

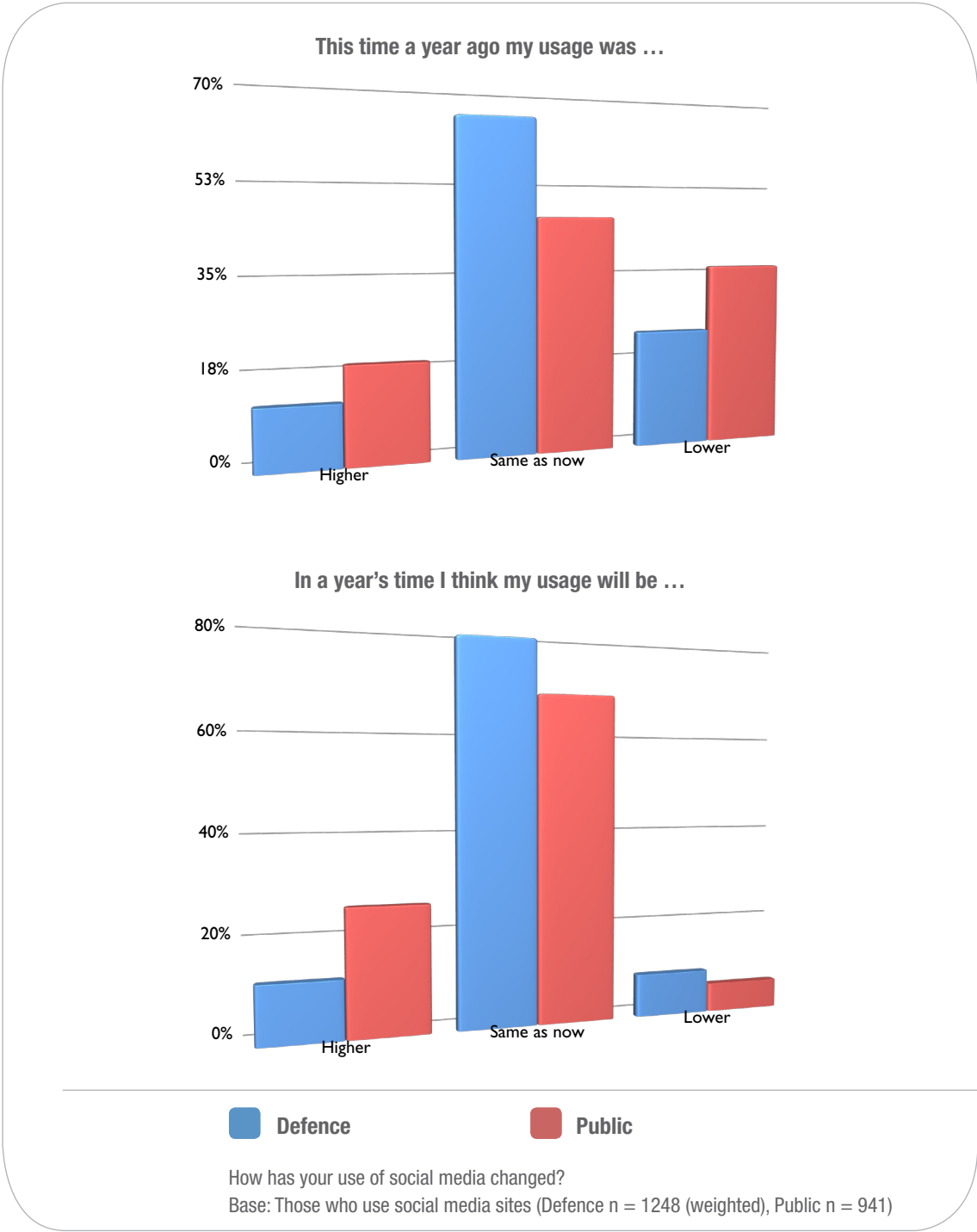


About how often would you say you use the following social media sites?
Base: Total respondents public n = 1000)

	Several times a day	Once a day	Every couple of days	Every week	Every month	Less often than every month	I don't use it	I've never heard of it
Myspace	1%	1%	2%	2%	3%	8%	80%	4%
foursquare	1%	1%	1%	1%	1%	1%	61%	33%
Flickr/Twitpic etc	1%	2%	3%	2%	4%	8%	62%	17%
LinkedIn	2%	2%	4%	6%	6%	6%	54%	19%
Blogs	4%	5%	8%	9%	8%	12%	47%	7%
Twitter	6%	4%	5%	3%	5%	6%	69%	2%
Youtube	6%	8%	18%	17%	15%	18%	18%	1%
Forums	6%	7%	9%	10%	10%	16%	36%	6%
Facebook	32%	19%	10%	9%	4%	6%	20%	0%

Facebook is even more popular among the general public: over 50% of public respondents claimed to visit the site every day. Overall usage levels for Facebook and YouTube are very similar; around 80% of respondents indicate that they visit the sites, but visits to the video sharing site are much less frequent.

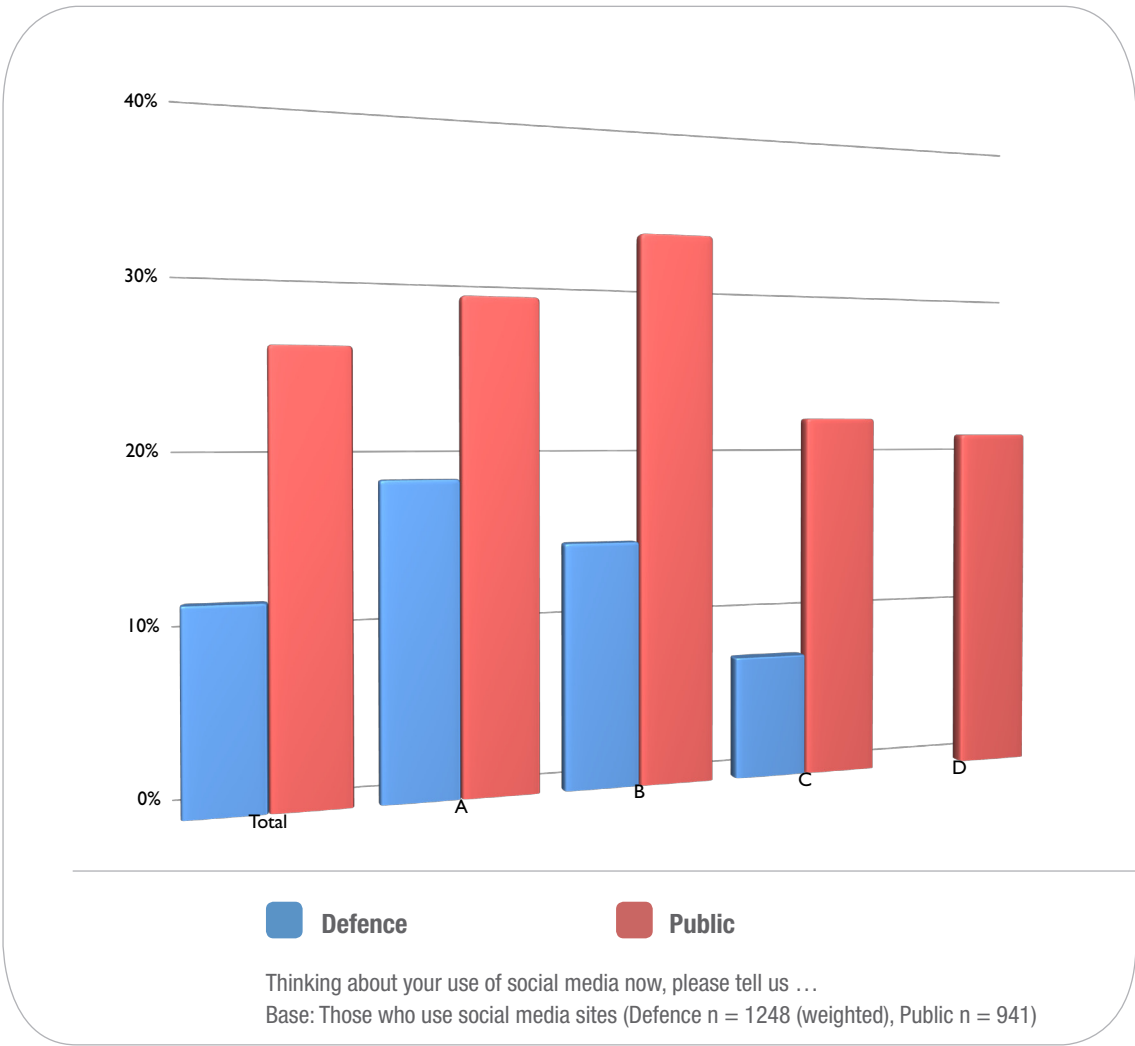
HOW HAS YOUR USE OF SOCIAL MEDIA CHANGED?



This time a year ago my usage was...	In a year's time I think my usage will be...	
	Defence	Public
Higher	12%	26%
Same as now	79%	68%
Lower	9%	6%

The majority of respondents, both in Defence and among the general public, feel that their usage will be unchanged in a year from now. However, around a quarter of Australians believe that their usage will increase, compared to just 12% of Defence employees.

IN A YEAR'S TIME MY USAGE WILL BE HIGHER....



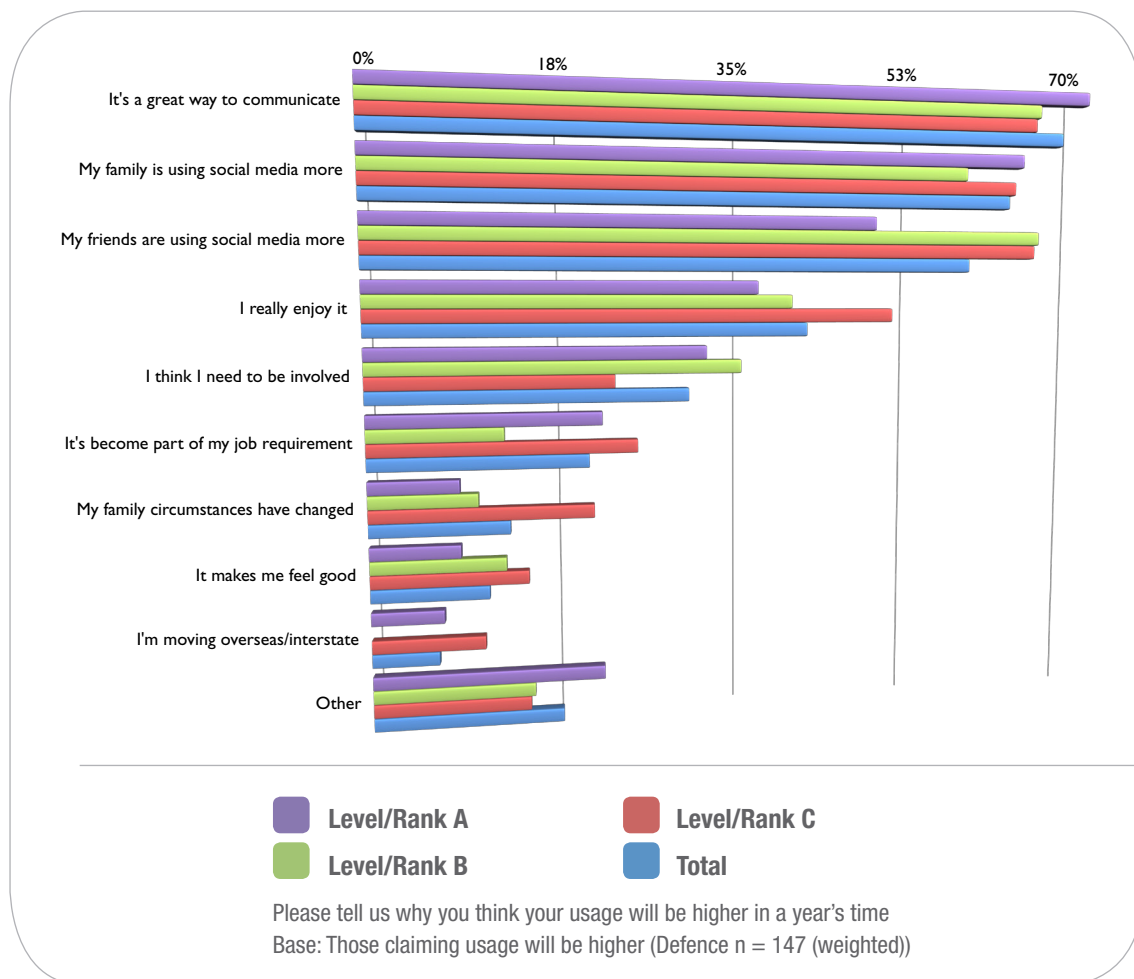
	Total	A	B	C	D
Defence	12%	18%	15%	7%	N/A
Public	26%	29%	33%	22%	21%

Eighteen per cent of Level/Rank A Defence employees feel that their social media usage will increase over the next year.

Conversely, only 7% of Level/Rank C employees feel the same way.

Among the general public, those in Group B were more likely to increase their usage. One in three of them believed they would be using social media more heavily this time next year.

WHY WILL YOUR USAGE BE HIGHER? DEFENCE EMPLOYEES



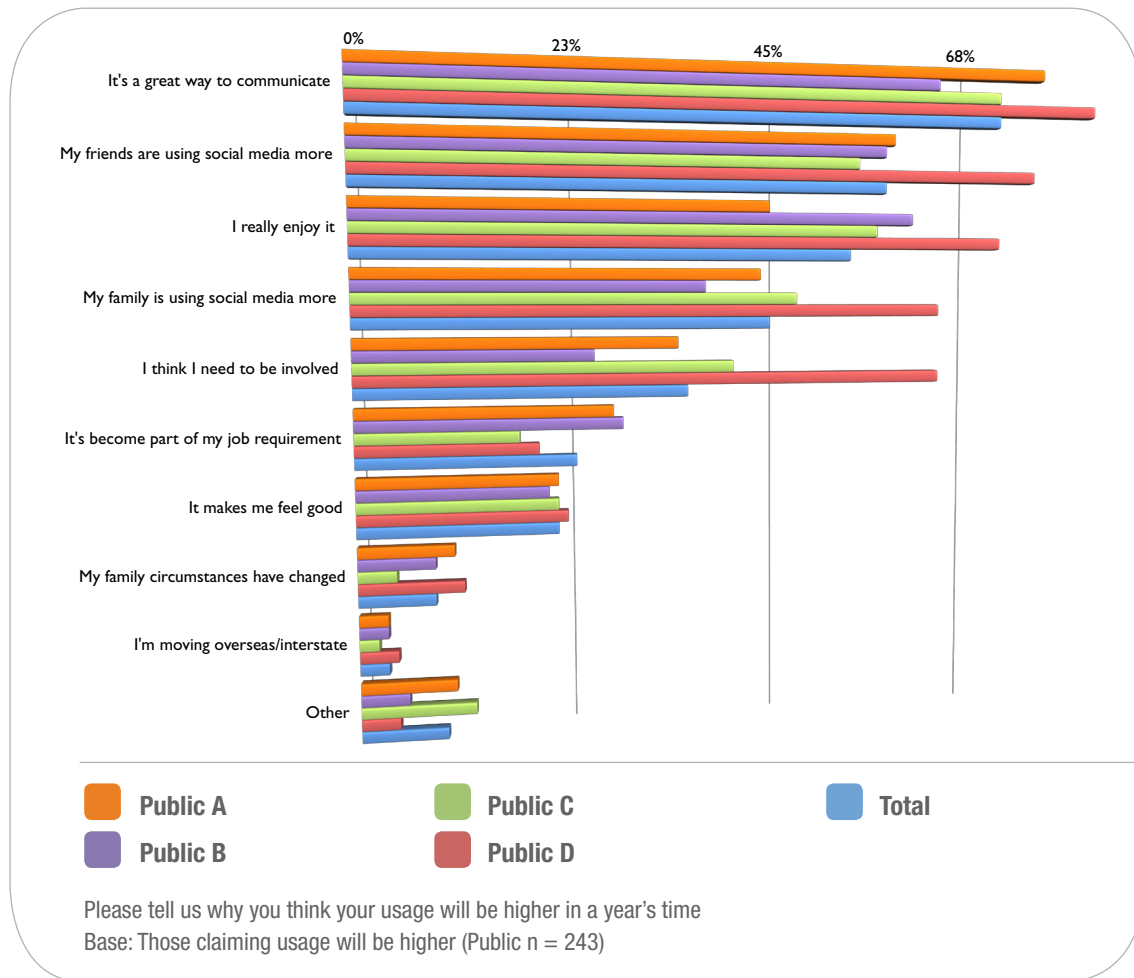
Please tell us why you think your usage will be higher in a year's time?	Total	Level/Rank A	Level/Rank B	Level/Rank C
Other	18%	22%	15%	15%
I'm moving overseas/interstate	6%	7%	0%	10%
It makes me feel good	11%	8%	13%	15%
My family circumstances have changed	13%	8%	10%	21%
It's become part of my job requirement	20%	22%	13%	25%
I think I need to be involved	30%	32%	35%	23%
I really enjoy it	42%	37%	40%	50%
My friends are using social media more	58%	48%	65%	65%
My family is using social media more	62%	63%	58%	63%
It's a great way to communicate	67%	70%	65%	65%

Respondents who feel that their usage of social media will increase cited communication as the biggest driver, particularly those at Level/Rank A.

Friends and family are also key reasons for increased use.

There is a feeling among those at Level/Rank A & B that they should become involved, perhaps in order to 'keep up'.

WHY WILL YOUR USAGE BE HIGHER? AUSTRALIAN PUBLIC



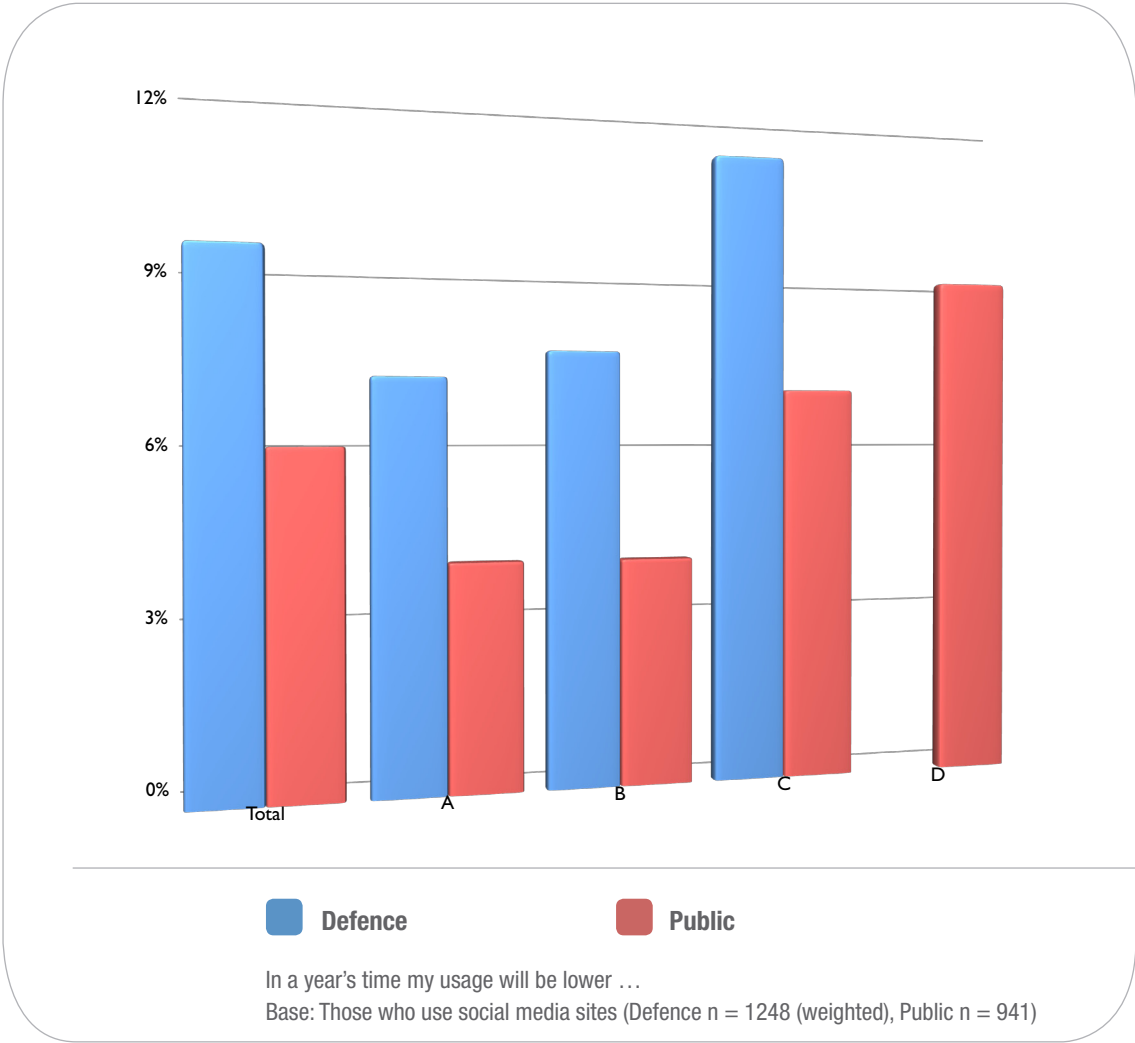
Q10b Please tell us why you think your usage will be higher in a year's time?	Total	Public A	Public B	Public C	Public D
Other	9%	10%	5%	12%	4%
I'm moving overseas/interstate	3%	3%	3%	2%	4%
My family circumstances have changed	8%	10%	8%	4%	11%
It makes me feel good	21%	21%	20%	21%	22%
It's become part of my job requirement	23%	27%	28%	17%	19%
I think I need to be involved	35%	34%	25%	40%	63%
My family is using social media more	44%	43%	37%	47%	63%
I really enjoy it	53%	44%	60%	56%	70%
My friends are using social media more	57%	58%	57%	54%	74%
It's a great way to communicate	70%	75%	63%	70%	81%

As with Defence employees, the general public feel that social media is a great way to communicate; hence their expected increase in use.

They are also finding that their friends and family are using social media more, too.

Over half of respondents claim that their enjoyment of social media will prompt an increase in usage.

IN A YEAR'S TIME MY USAGE WILL BE LOWER...



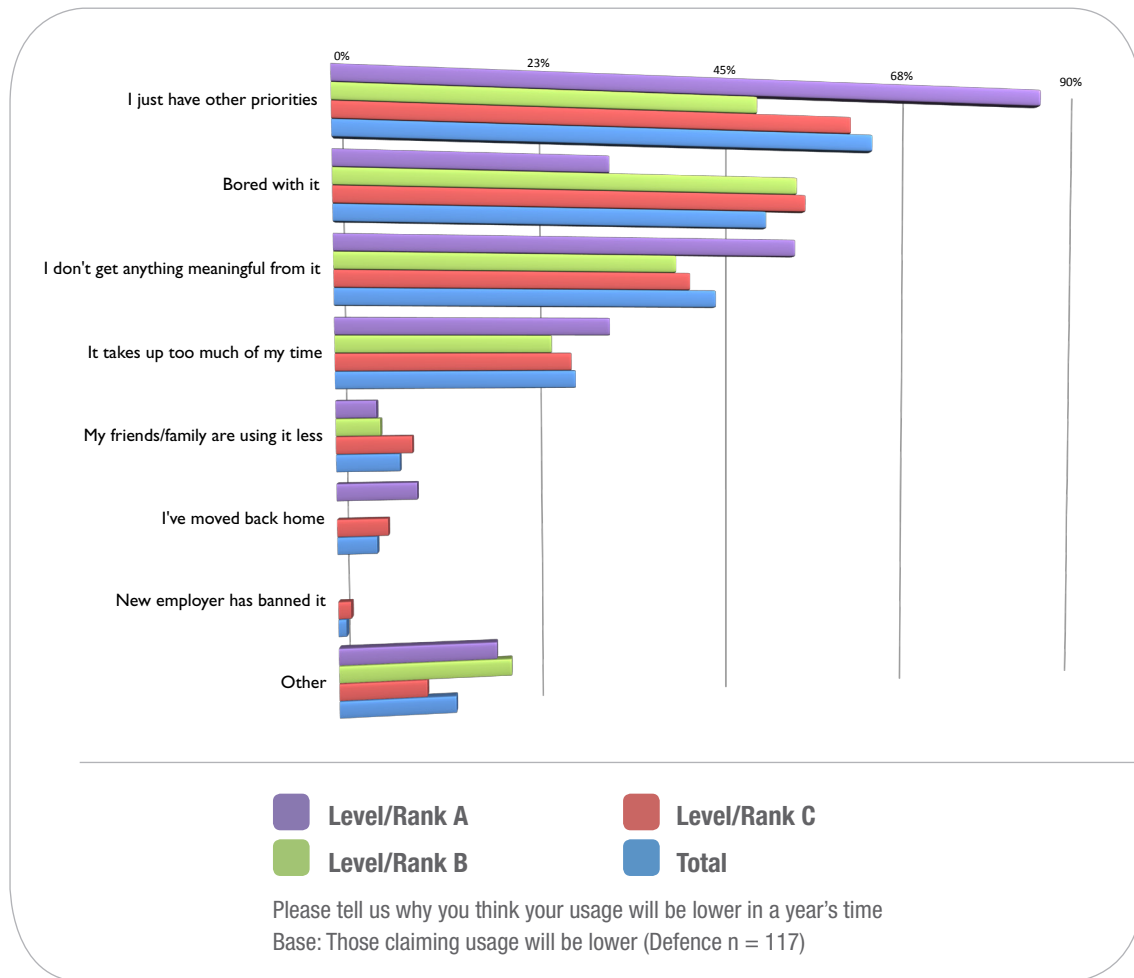
	Total	A	B	C	D
Defence	9%	7%	8%	11%	N/A
Public	6%	4%	4%	7%	9%

Only 7% of Level/Rank A Defence employees believe they will be using social media less than they do now come next year.

This figure rises slightly to 8% for Level/Rank B and 11% for Level/Rank C.

There is a similar pattern among the general public. Just 4% of Group A & B respondents indicated that their usage will be less, rising to 7% for Group C.

WHY WILL YOUR USAGE BE LOWER? DEFENCE FORCE

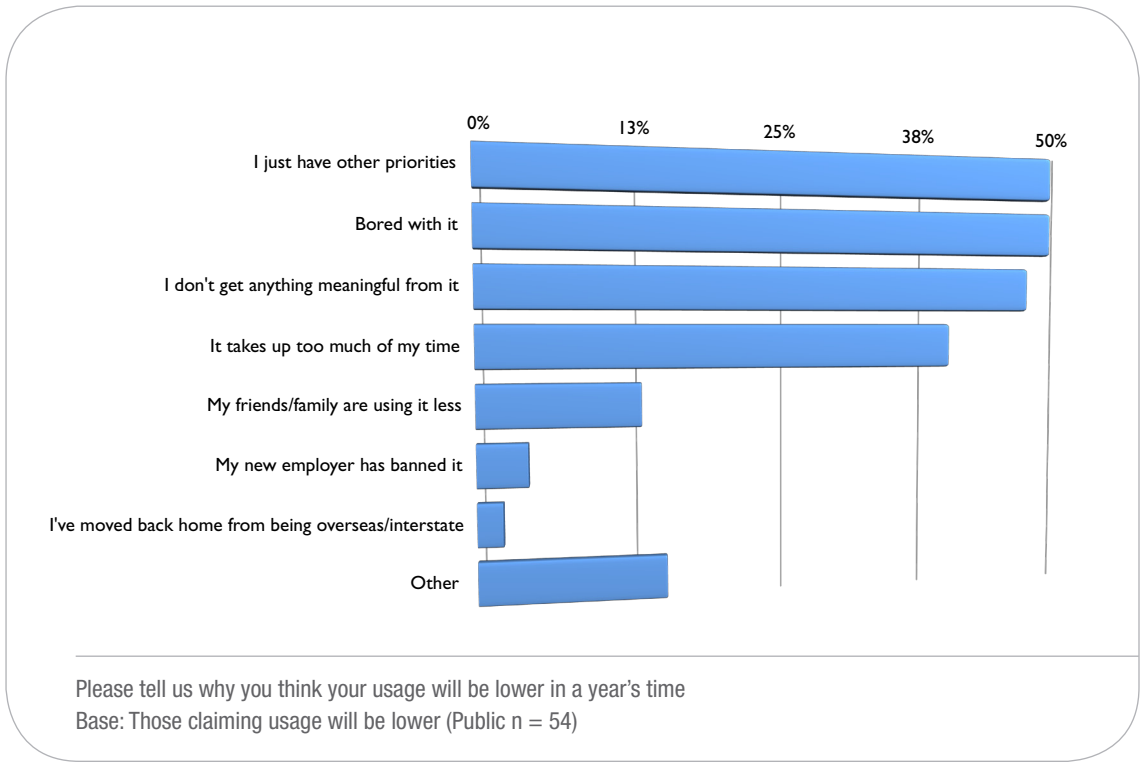


	Total	Level/Rank A	Level/Rank B	Level/Rank C
Other	13%	17%	19%	10%
New employer has banned it	1%	0%	0%	1%
I've moved back home	4%	9%	0%	5%
My friends/family are using it less	7%	4%	5%	8%
It takes up too much of my time	27%	30%	24%	26%
I don't get anything meaningful from it	43%	52%	38%	40%
Bored with it	49%	30%	52%	53%
I just have other priorities	62%	83%	48%	59%

The single biggest reason for a drop in social media usage is other priorities, particularly among Level/Rank A respondents. Over 80% of them indicate that this is why their usage will be less in a year's time.

Around half of all respondents claim to be bored with social media, although this is less of an issue for those at Level/Rank A, who are more likely to agree that they don't get anything meaningful from it.

WHY WILL YOUR USAGE BE LOWER? AUSTRALIAN PUBLIC

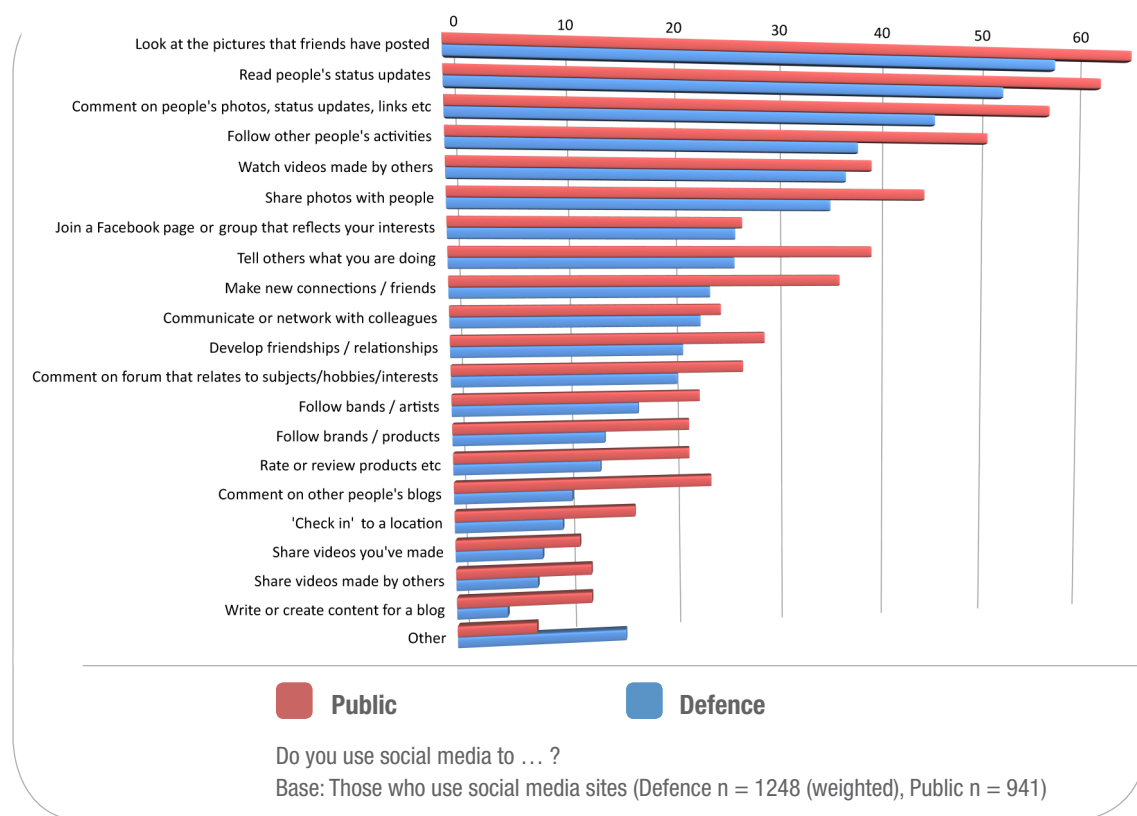


	Total
Other	15%
I've moved back home from being overseas/interstate	2%
My new employer has banned it	4%
My friends/family are using it less	13%
It takes up too much of my time	39%
I don't get anything meaningful from it	46%
Bored with it	48%
I just have other priorities	48%

As with Defence employees, the main reasons given for a drop in social media usage are other priorities and boredom.

Almost half of all respondents feel that they do not get anything meaningful from it and 39% believe it takes up too much time.

DO YOU USE SOCIAL MEDIA TO...?

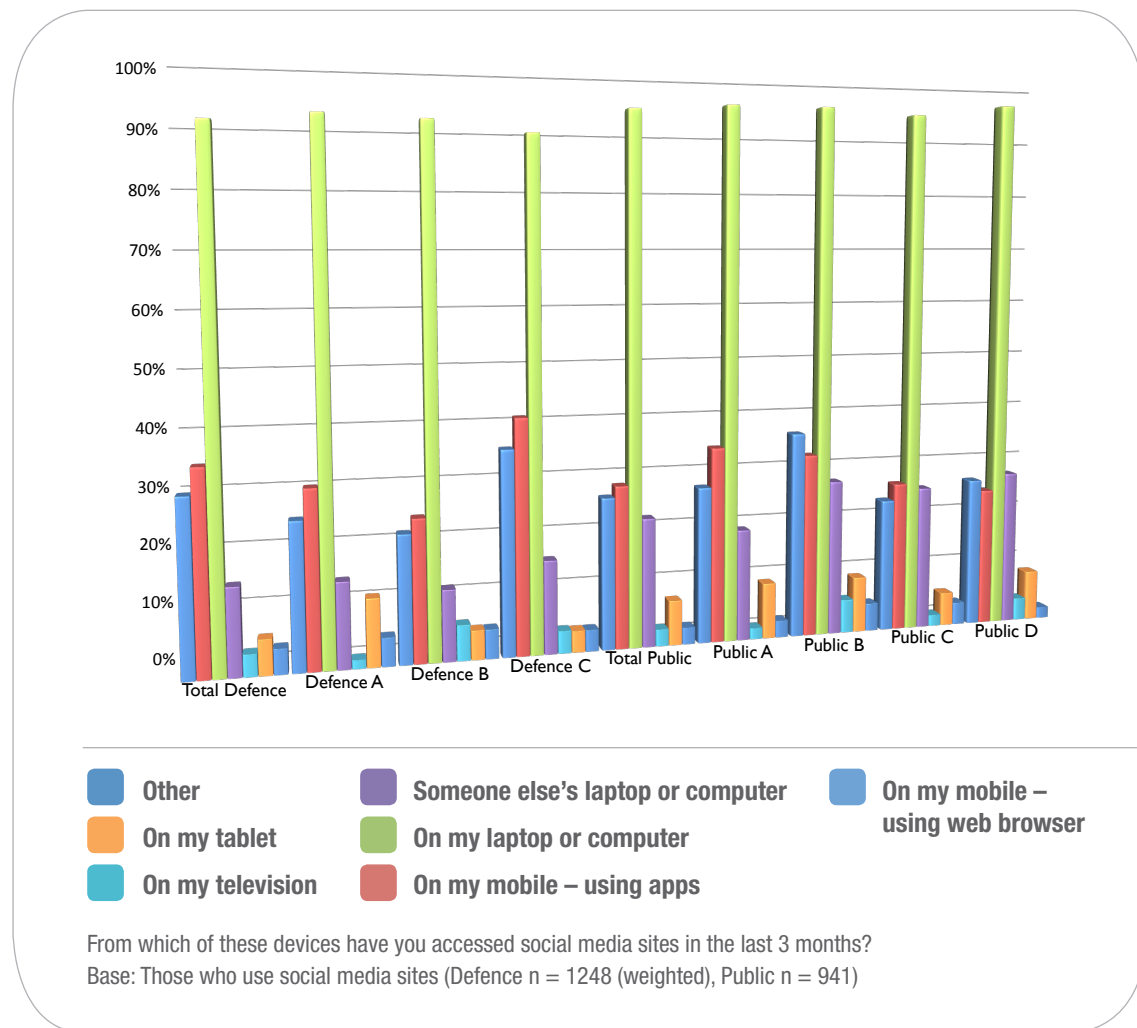


	Defence	Public
Other	15%	7%
Write or create content for a blog	4%	12%
Share videos made by others	7%	12%
Share videos you've made	8%	11%
'Check in' to a location	10%	16%
Comment on other people's blogs	10%	23%
Rate or review products etc	13%	21%
Follow brands / products	13%	21%
Follow bands / artists	16%	22%
Comment on forum that relates to subjects/hobbies/interests	20%	26%
Develop friendships / relationships	21%	28%
Communicate or network with colleagues	22%	24%
Make new connections / friends	23%	35%
Tell others what you are doing	25%	38%
Join a Facebook page or group that reflects your interests	25%	26%
Share photos with people	34%	43%
Watch videos made by others	36%	38%
Follow other people's activities	37%	49%
Comment on people's photos, status updates, links etc	44%	55%
Read people's status updates	50%	60%
Look at the pictures that friends have posted	55%	63%

Reasons for using social media do not appear to differ much between those in Defence and the general public.

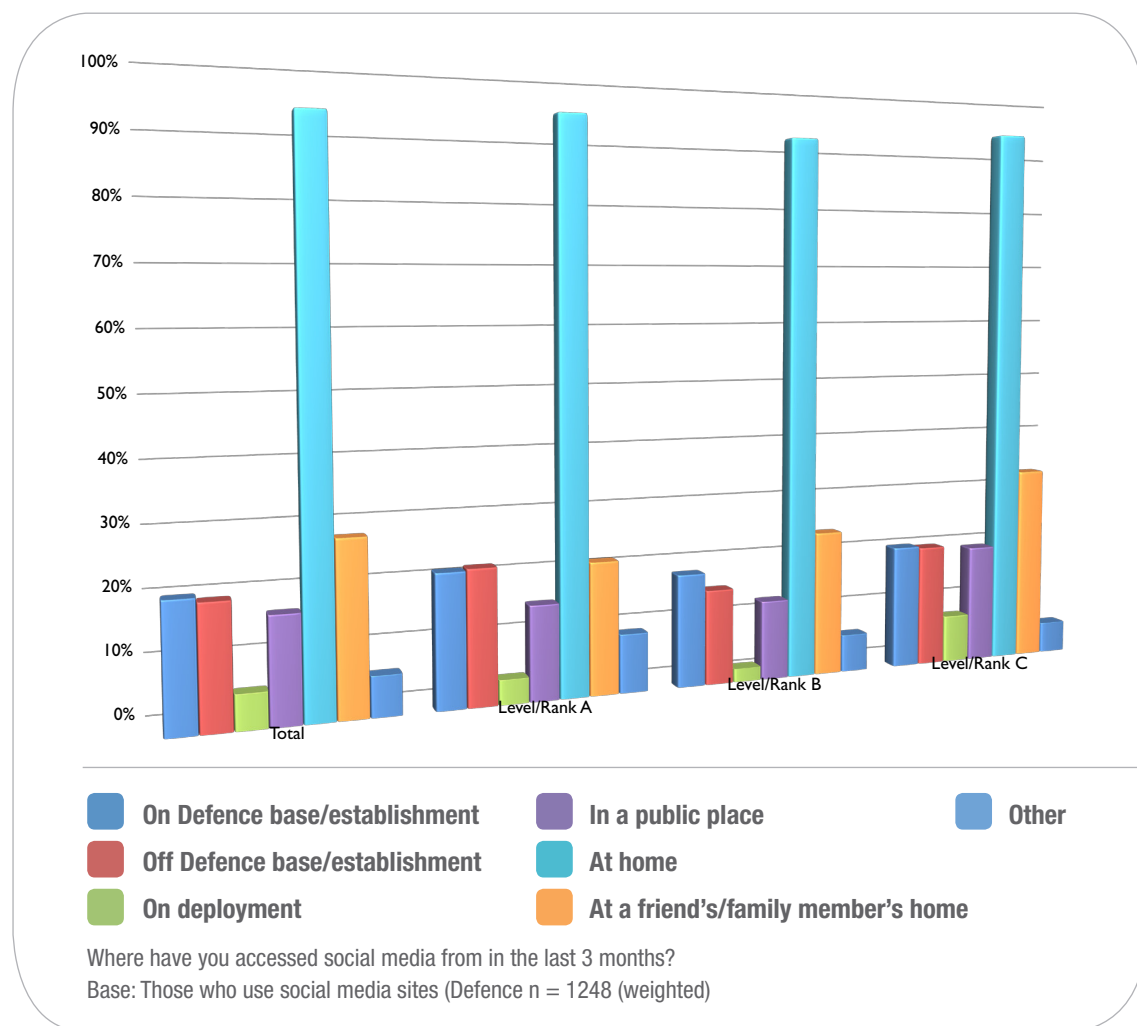
For both groups of respondents, the most common activity is looking at pictures that friends have posted, followed closely by reading and commenting on people's status updates and photos.

DEVICES USED TO ACCESS SOCIAL MEDIA



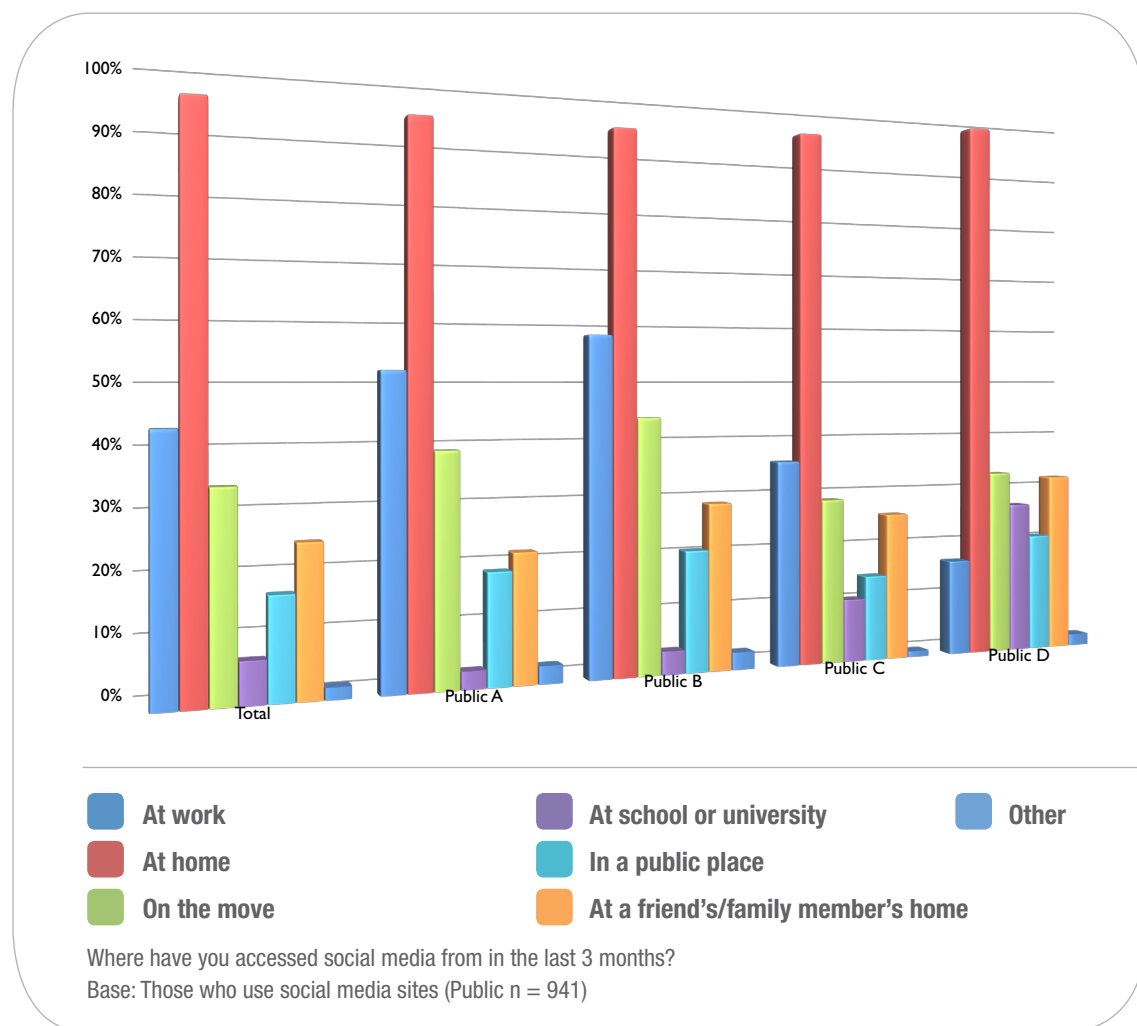
The vast majority of respondents accessed social media sites on their personal laptop or computer. Access via mobiles is highest among Defence Level/Rank C respondents, of whom 42% social media via apps for access and 36% use their mobile phone's web browser. Interestingly, their mobile app usage is considerably higher than that of any of the public groups. The general public are more open to using someone else's computer than Defence employees, who perhaps have stronger concerns about security.

LOCATIONS ACCESSED SOCIAL MEDIA FROM DEFENCE



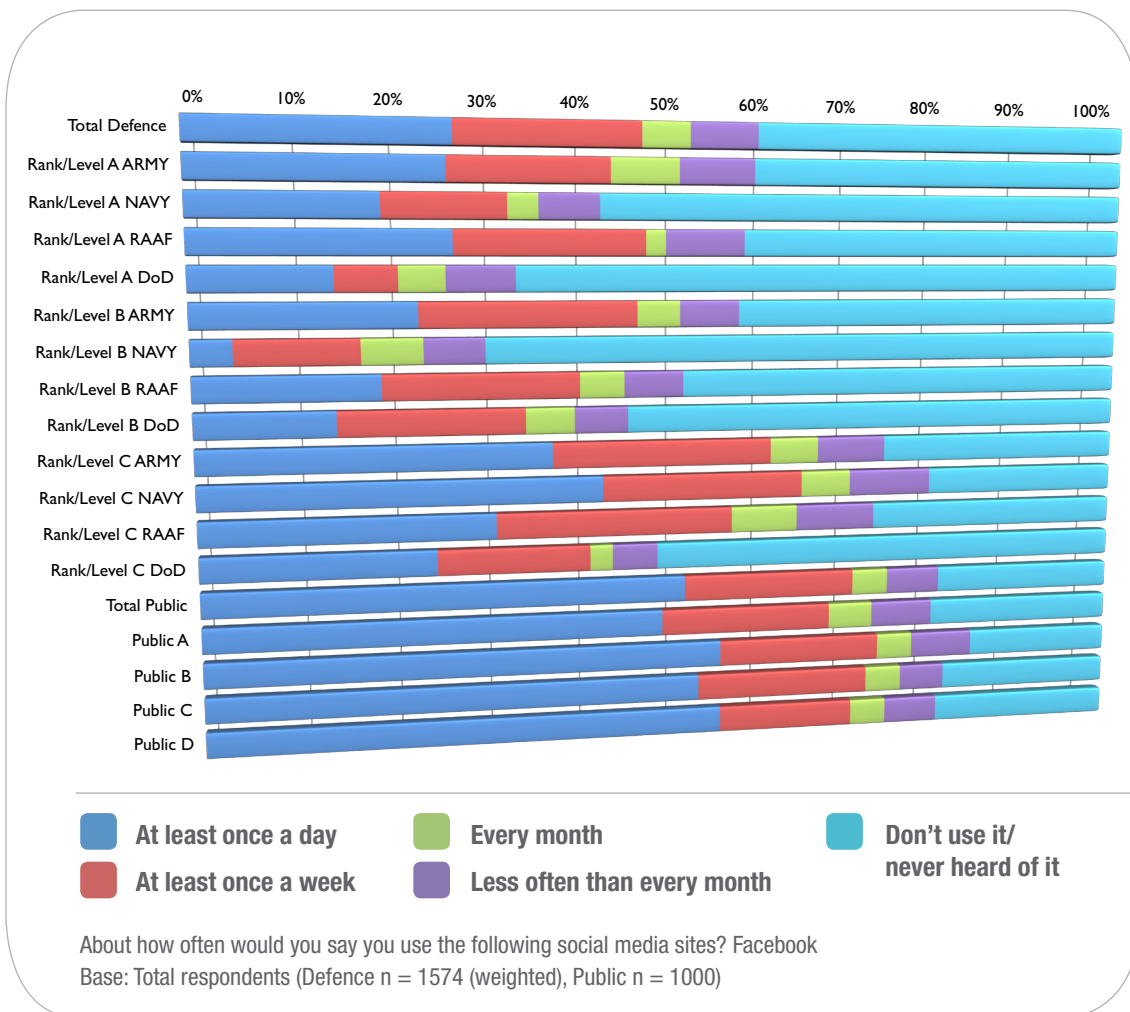
Level/Rank C Defence employees have a far greater propensity than either Level/Rank A or B to access social media at a friend's or family member's home or in public. This could be because they are less worried about security than those more senior.

LOCATIONS ACCESSED SOCIAL MEDIA FROM PUBLIC



As with Defence employees, the general public are most likely to access social media from home. However, over half of Level A & B respondents indicated that they would also use social media at work, compared to just 36% of Level C respondents, who may be less likely to have access to a computer at work.

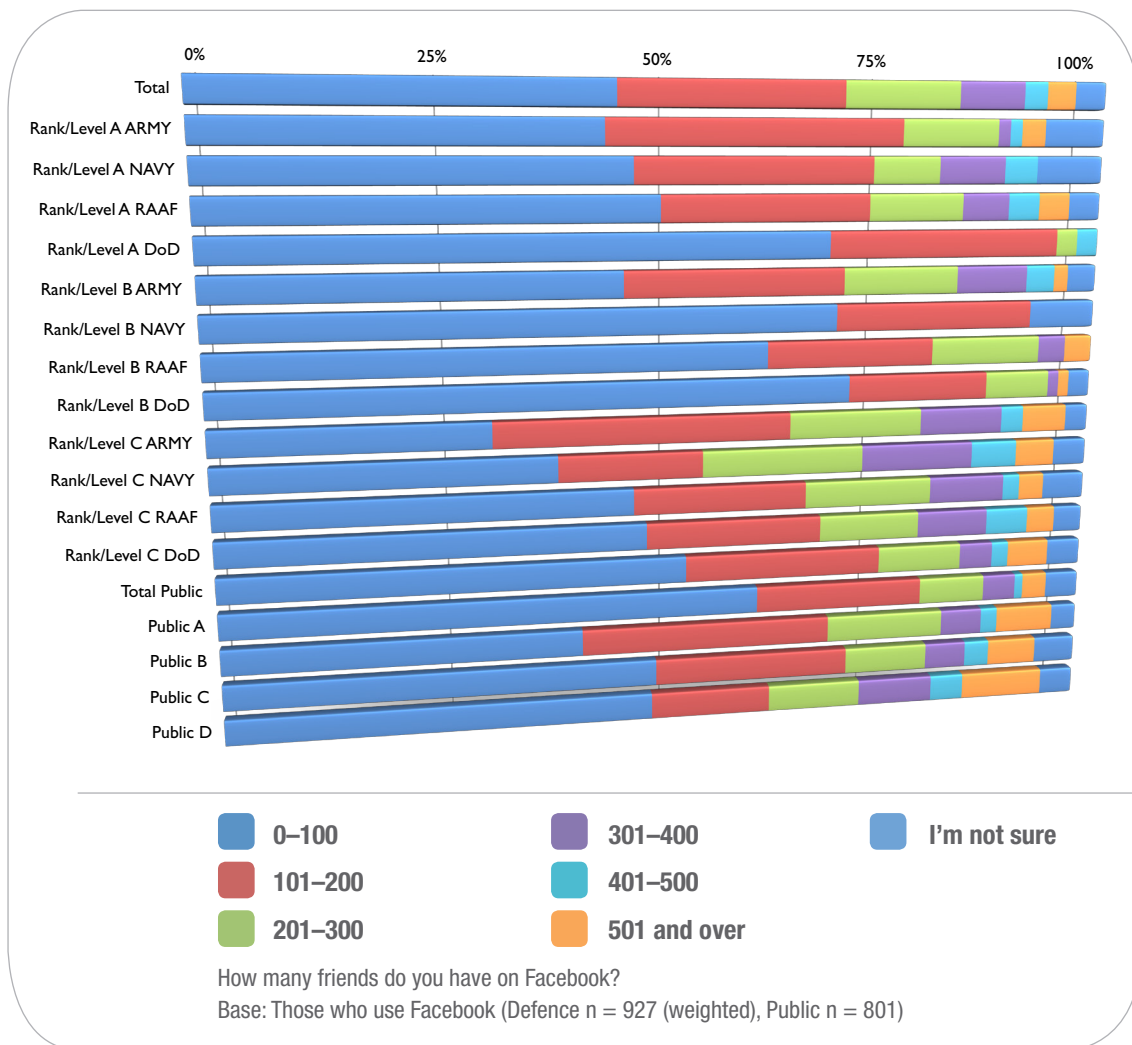
HOW OFTEN DO YOU USE FACEBOOK?



	Defence Total	A Army	A NAVY	A RAAF	A DoD	B Army	B Navy	B RAAF	B DoD	C ARMY	C NAVY	C RAAF	C DoD	Public Total	Public A	Public B	Public C	Public D
At least once a day	27%	26%	20%	27%	15%	23%	4%	19%	14%	37%	42%	30%	24%	51%	49%	55%	52%	55%
At least once a week	20%	17%	13%	20%	6%	23%	13%	21%	19%	24%	22%	25%	16%	19%	19%	18%	19%	15%
Every month	5%	7%	3%	2%	5%	5%	7%	5%	5%	5%	5%	7%	2%	4%	5%	4%	4%	4%
Less often than every month	7%	8%	7%	9%	7%	6%	7%	6%	6%	8%	9%	9%	5%	6%	7%	7%	5%	6%
Don't use it/never heard of it	41%	42%	59%	43%	67%	44%	72%	50%	55%	27%	21%	28%	52%	20%	21%	16%	19%	20%

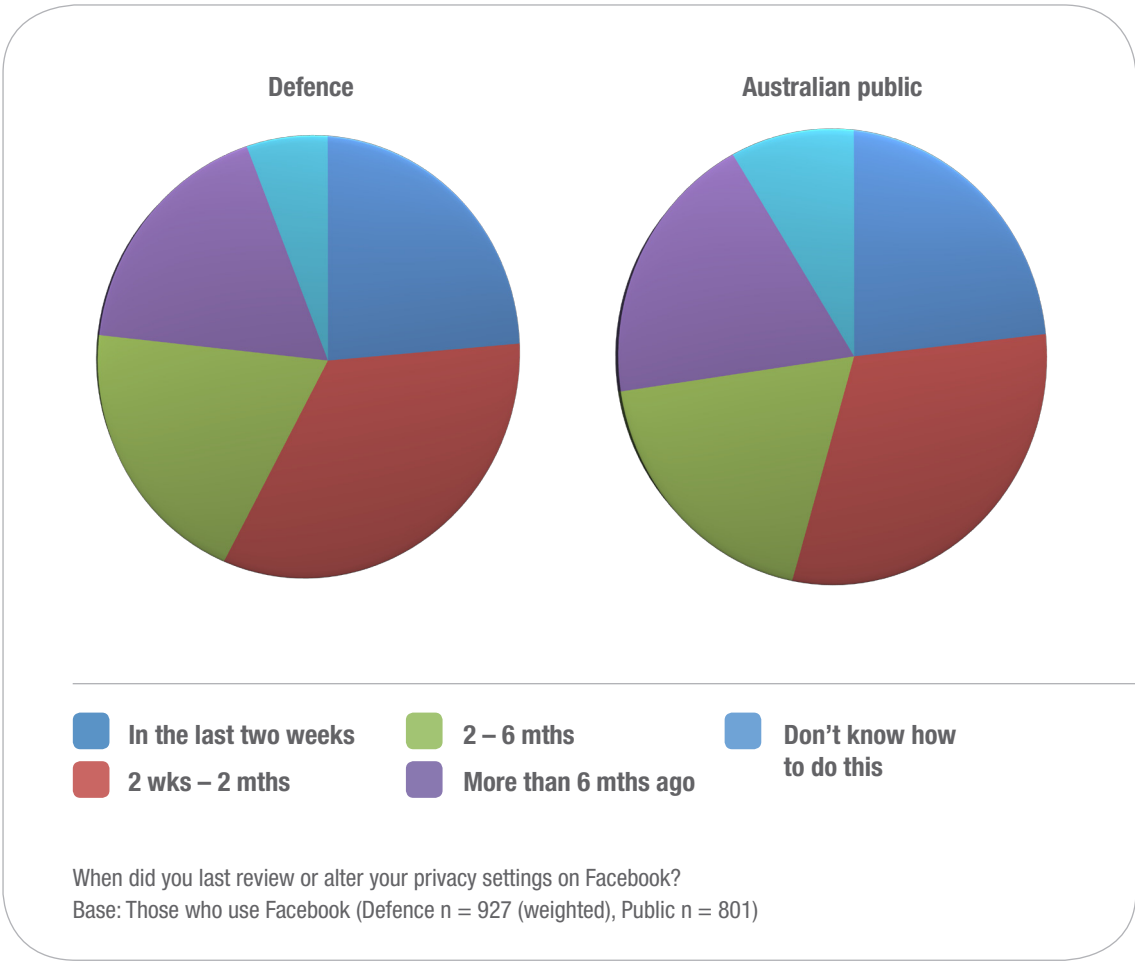
While Facebook usage is fairly consistent across all four of the public groups, there are considerable differences within Defence, Overall Level/Rank C respondents claim the highest usage (although DoD employees use it considerably less than their Army/Navy/RAAF colleagues). The group with the fewest regular Facebook users is B Navy, of whom only 4% indicate that they access Facebook daily and around 7 in 10 claim not to use it at all.

HOW MANY FRIENDS DO YOU HAVE ON FACEBOOK?



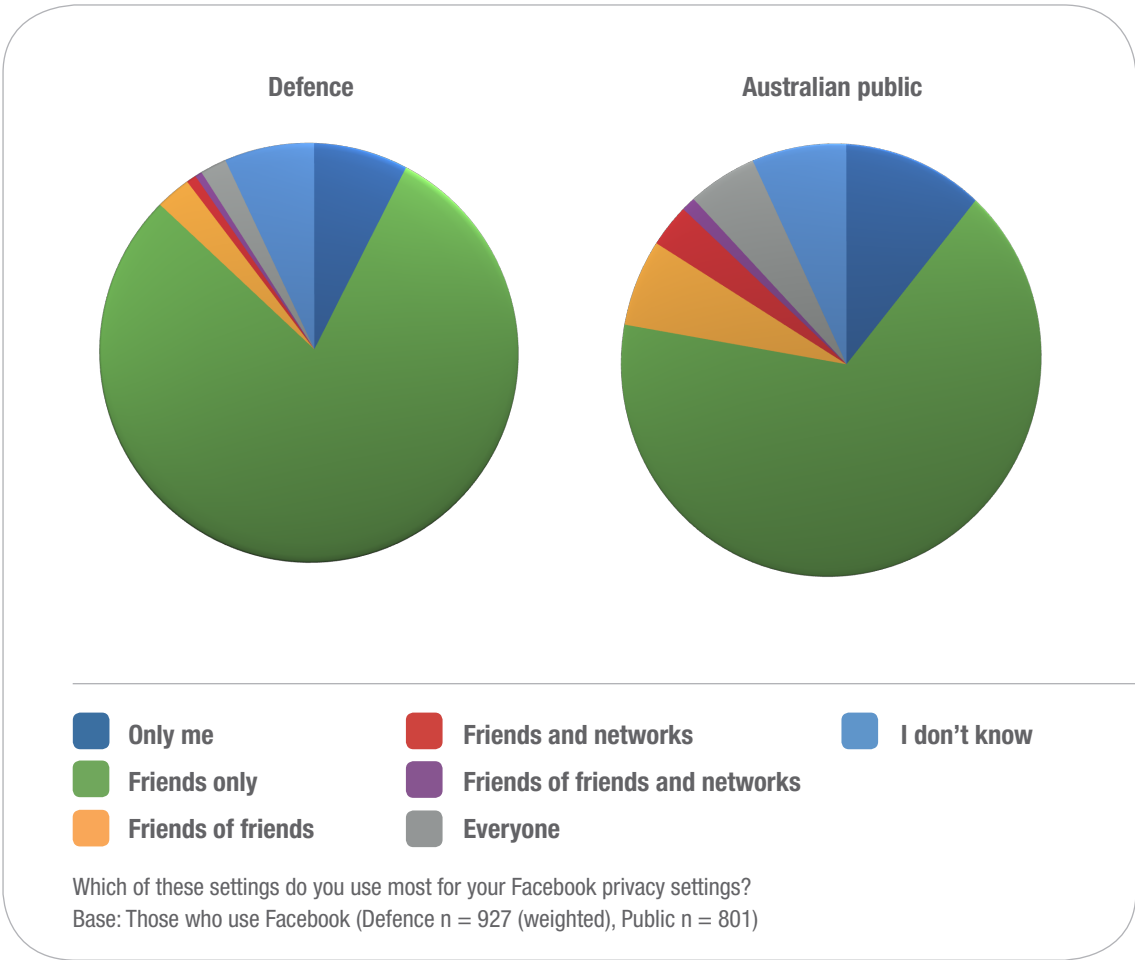
Frequency of Facebook usage appears to correlate directly with the number of Facebook friends. Those who use the site less frequently are more likely to have fewer friends. Defence Level/Rank C respondents have the highest number of friends, particularly those in the Navy.

WHEN DID YOU LAST REVIEW YOUR PRIVACY SETTINGS ON FACEBOOK?



When it comes to security settings, there is little difference between Defence employees and the Australian public. Over half of all respondents reviewed their privacy settings in the last two months, and under 10% said they were unsure of how to do this.

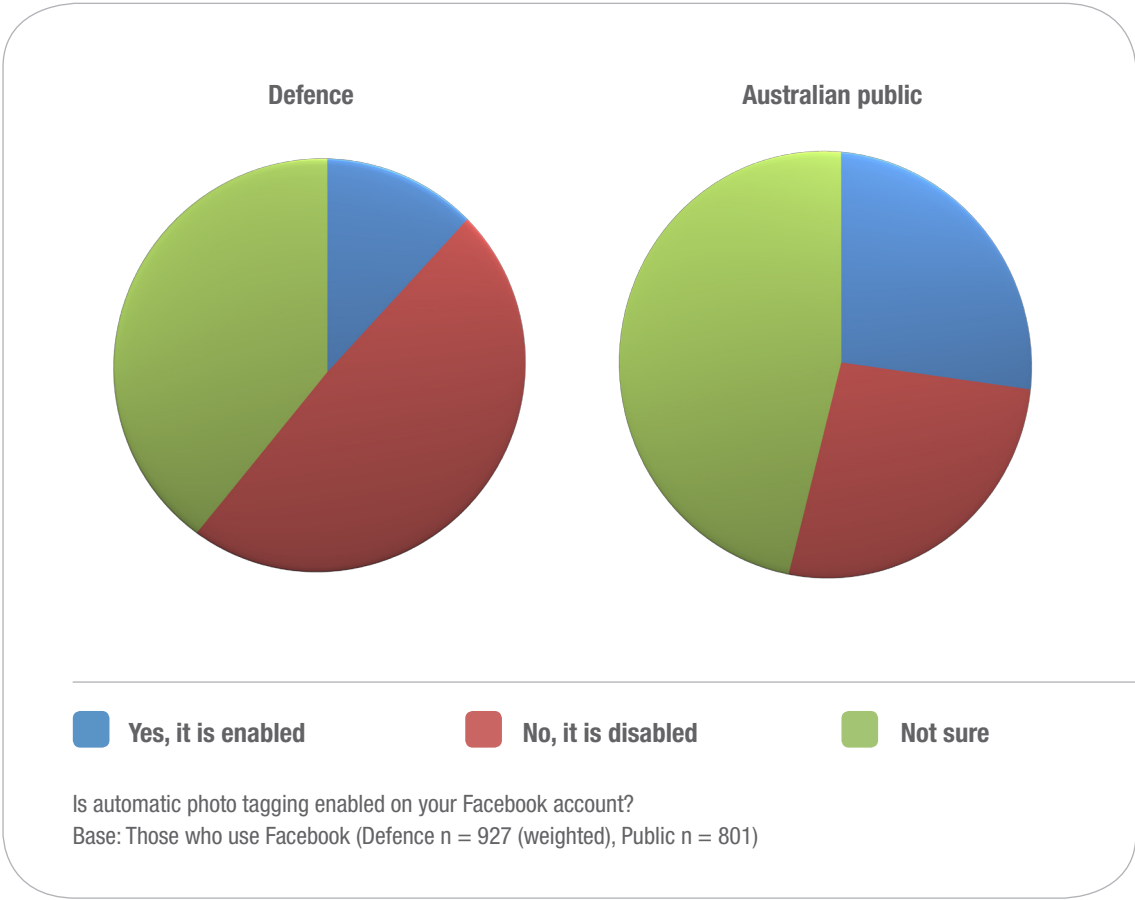
WHICH FACEBOOK PRIVACY SETTING DO YOU USE MOST?



	Defence	Public
Only me	7%	11%
Friends only	80%	67%
Friends of friends	3%	6%
Friends and networks	1%	3%
Friends of friends and networks	1%	1%
Everyone	2%	5%
I don't know	7%	7%

The vast majority of Defence employees have their Facebook set to ‘Friends Only’. The general public are a little more likely to open up their Facebook to ‘Friends of friends’ and ‘Friends of friends and networks’.

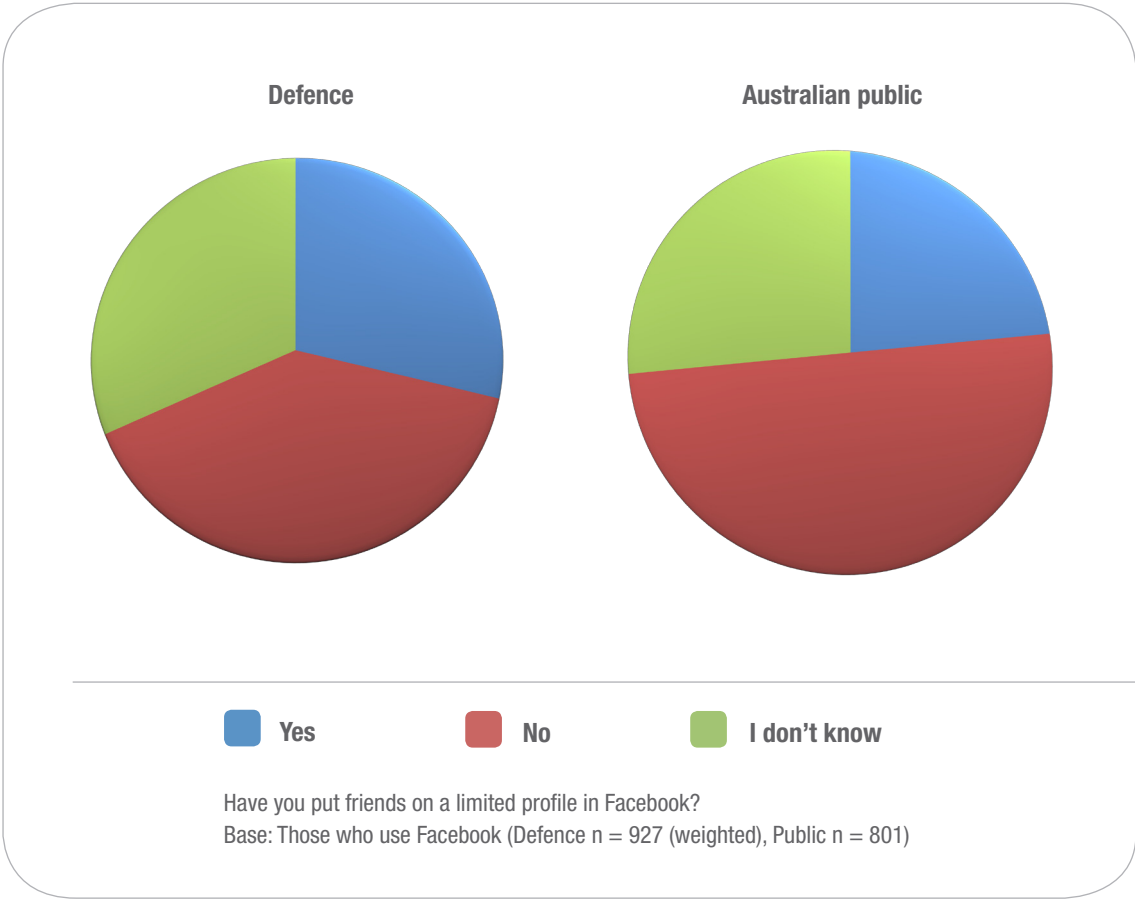
IS AUTOMATIC PHOTO TAGGING ENABLED?



	Defence	Public
Yes, it is enabled	12%	27%
No, it is disabled	49%	27%
Not sure	39%	46%

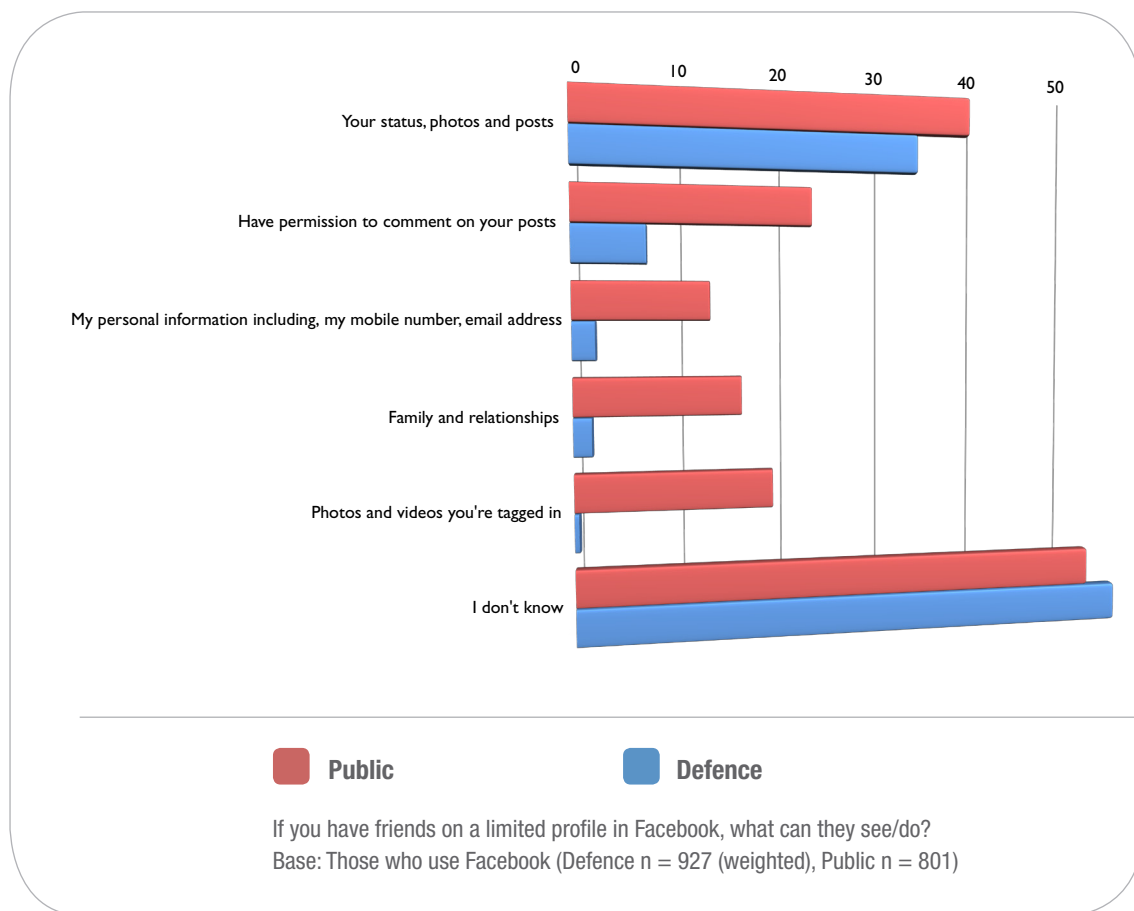
It appears that Defence employees are more savvy than the general public when it comes to photo tagging. Almost half of the general public are unsure as to whether or not they have automatic tagging enabled or not, compared to just 36% of Defence employees. Furthermore, of those who are aware of this feature, only 12% of Defence employees have activated it, compared to over a quarter of the public respondents.

HAVE YOU PUT FRIENDS ON A LIMITED PROFILE?



Twenty-nine per cent of Defence employees have put Facebook friends on a limited profile, compared to 23% of the general public.

IF YOU HAVE FRIENDS ON A LIMITED PROFILE IN FACEBOOK, WHAT CAN THEY SEE/DO?

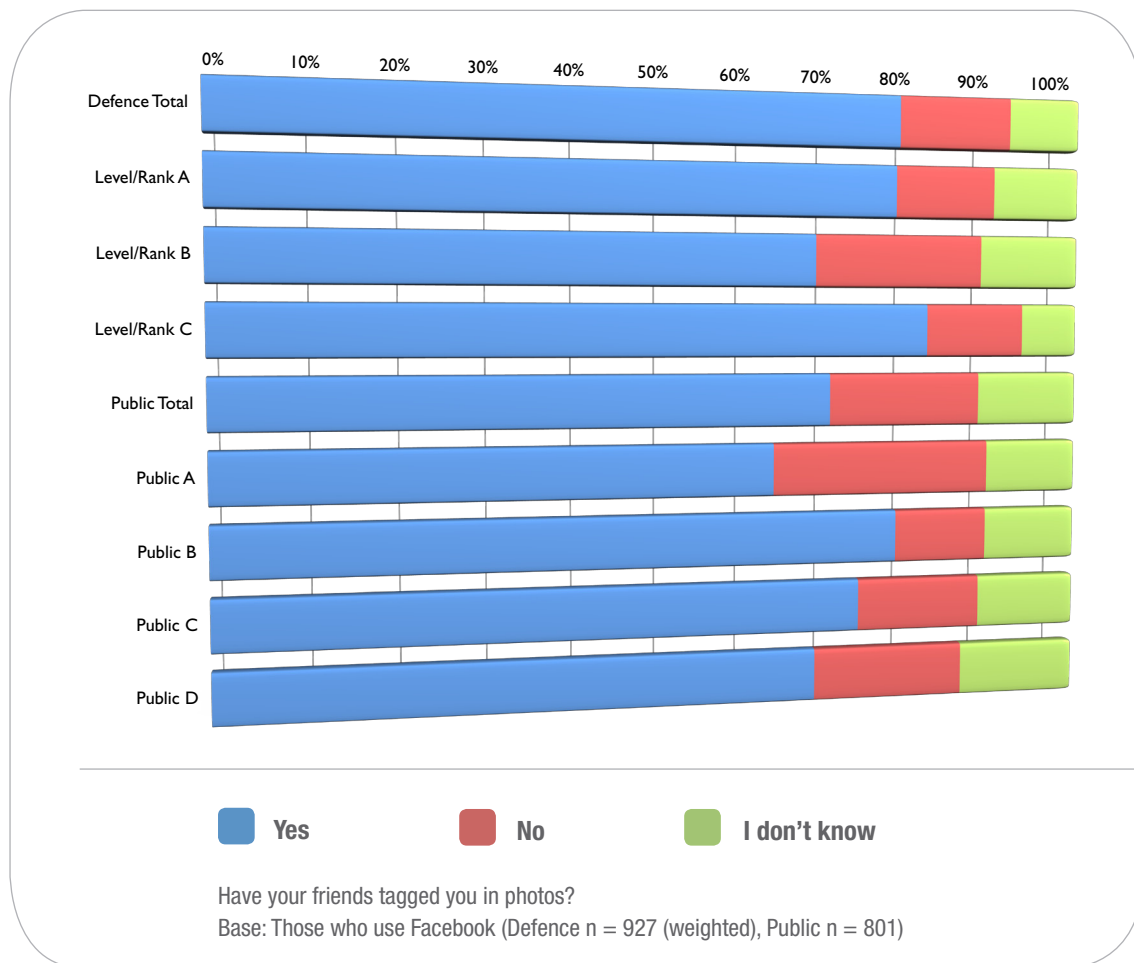


	Defence	Public
I don't know	55%	52%
Photos and videos you're tagged in	0%	19%
Family and relationships	2%	16%
My personal information, including my mobile number, email address	2%	13%
Have permission to comment on your posts	7%	23%
Your status, photos and posts	34%	39%

Thirty-nine per cent of the general public and 34% of Defence employees indicated that friends on a limited profile can see their status, photos and posts.

However, Defence personnel are less likely than the general public to give their limited profile friends permission to comment on their posts or see their personal information.

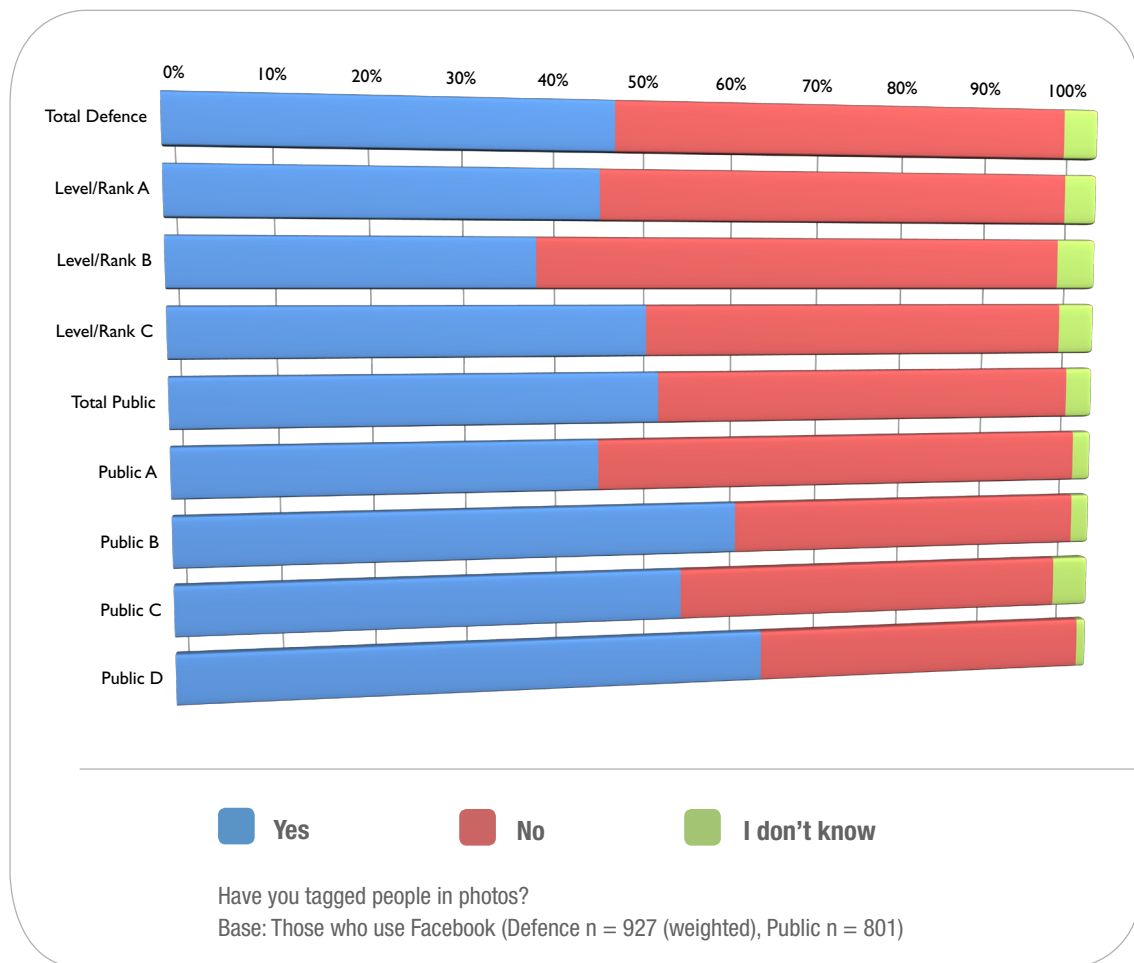
HAVE YOUR FRIENDS TAGGED YOU IN PHOTOS?



	Defence Total	Level/ Rank A	Level/ Rank B	Level/ Rank C	Public Total	Public A	Public B	Public C	Public D
Yes	78%	78%	68%	81%	69%	63%	77%	74%	68%
No	13%	12%	20%	12%	18%	26%	11%	15%	18%
I don't know	9%	10%	12%	7%	12%	11%	11%	12%	14%

Over three-quarters of Facebook users in Defence have been tagged in a photo, compared to just 69% of the general public. Among Defence employees, Level/Rank C respondents were most likely to have been tagged.

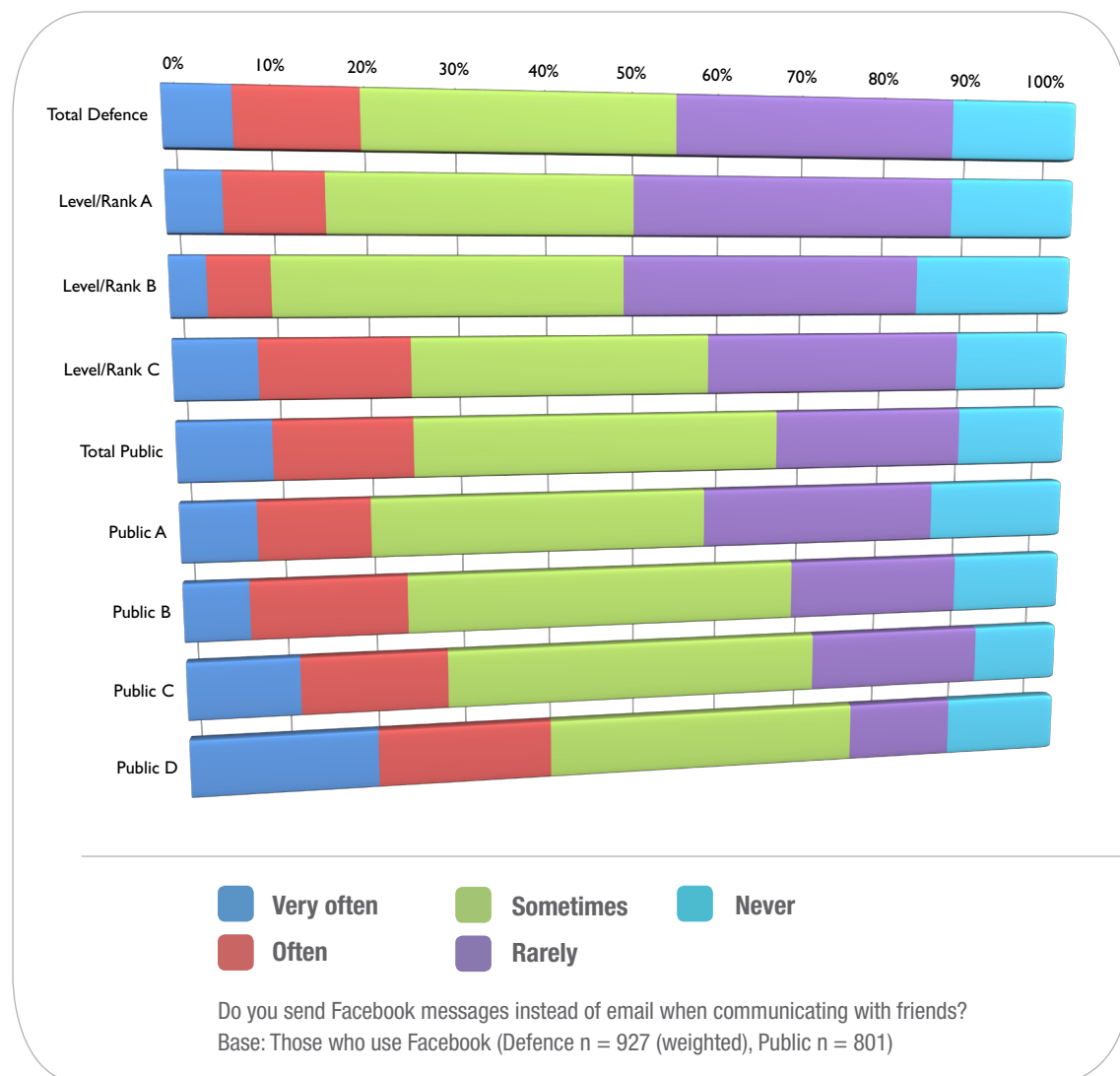
HAVE YOU TAGGED PEOPLE IN PHOTOS?



	Defence Total	Level/ Rank A	Level/ Rank B	Level/ Rank C	Public Total	Public A	Public B	Public C	Public D
Yes	46%	44%	38%	49%	51%	44%	59%	53%	62%
No	50%	52%	58%	47%	47%	54%	39%	43%	37%
I don't know	4%	4%	4%	4%	3%	2%	2%	4%	1%

Forty-six per cent of Defence respondents have tagged people in photos, compared to 51% of the general public. Level/Rank C Defence employees were considerably more likely than their Level/Rank A and B colleagues to tag photos.

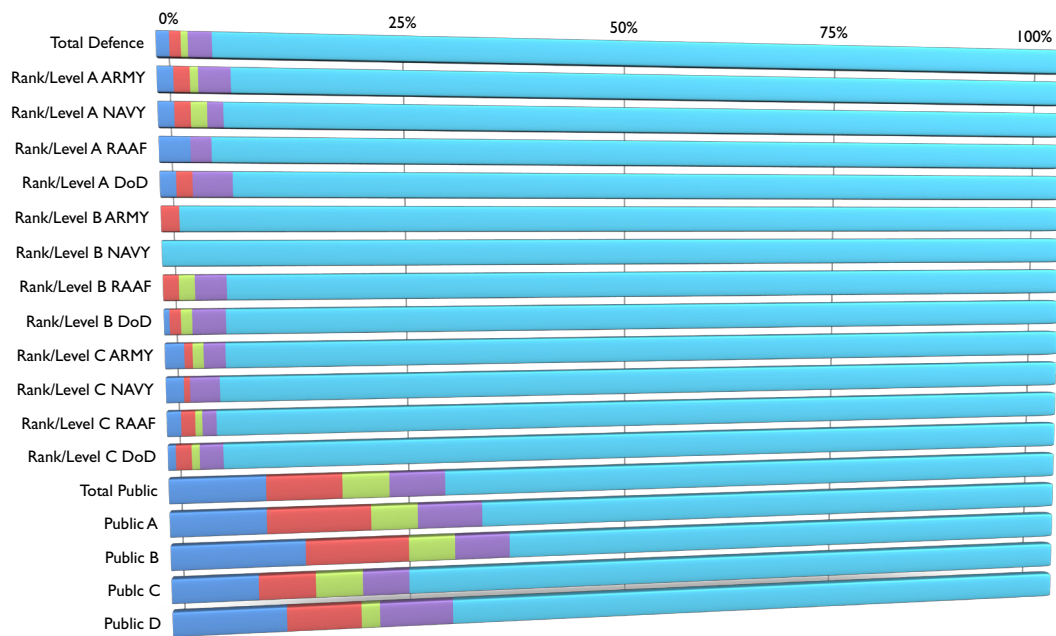
DO YOU SEND FACEBOOK MESSAGES INSTEAD OF EMAIL?



	Defence Total	Level/ Rank A	Level/ Rank B	Level/ Rank C	Public Total	Public A	Public B	Public C	Public D
Very often	7%	6%	4%	9%	10%	8%	7%	12%	20%
Often	13%	10%	7%	16%	15%	12%	17%	16%	19%
Sometimes	34%	33%	38%	33%	41%	37%	44%	42%	35%
Rarely	32%	36%	34%	29%	22%	27%	20%	20%	12%
Never	15%	15%	18%	13%	13%	16%	13%	10%	13%

Just over half of all Defence employees send Facebook messages instead of email at least sometimes. This compares to around two-thirds for the general public. Group C for both Defence and the public have a greater propensity to send Facebook messages than their Group A and B counterparts.

HOW OFTEN DO YOU USE TWITTER?



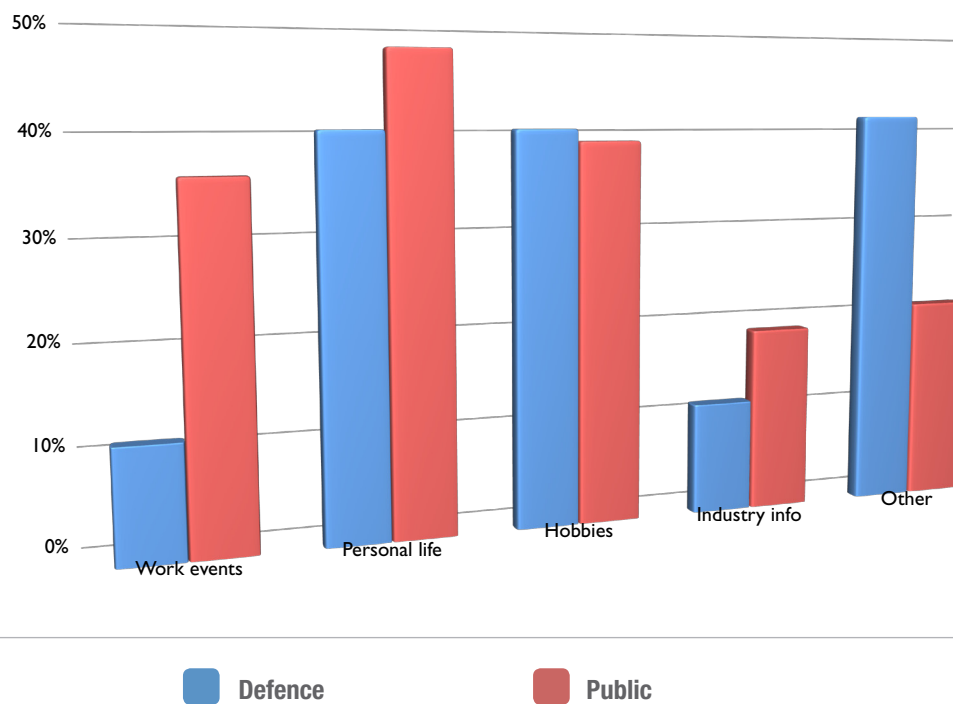
■ At least once a day
 ■ Every month
 ■ At least once a week
 ■ Less often than every month
 ■ Don't use it/never heard of it

About how often would you say you use the following social media sites? Twitter
 Base: Total respondents (Defence n = 1574 (weighted), Public n = 1000)

	Defence Total	A Army	A NAVY	A RAAF	A DoD	B Army	B Navy	B RAAF	B DoD	C ARMY	C NAVY	C RAAF	C DoD	Public Total	Public A	Public B	Public C	Public D
At least once a day	1%	2%	2%	3%	2%	0%	0%	0%	1%	2%	2%	1%	1%	10%	10%	14%	9%	12%
At least once a week	1%	2%	2%	0%	2%	2%	0%	2%	1%	1%	1%	1%	2%	8%	11%	11%	6%	8%
Every month	1%	1%	2%	0%	0%	0%	0%	2%	1%	1%	0%	1%	1%	5%	5%	5%	5%	2%
Less often than every month	2%	3%	2%	2%	4%	0%	0%	3%	3%	2%	3%	1%	2%	6%	7%	6%	5%	8%
Don't use it/never heard of it	94%	93%	93%	96%	92%	98%	100%	94%	94%	94%	95%	95%	94%	71%	67%	64%	75%	71%

Twitter usage is very low across all levels/ranks within Defence, within which less than 6% of any one group indicate that they visit the site. Usage among the general public is considerably higher, but still nowhere near Facebook levels.

WHAT DO YOU TWEET ABOUT?



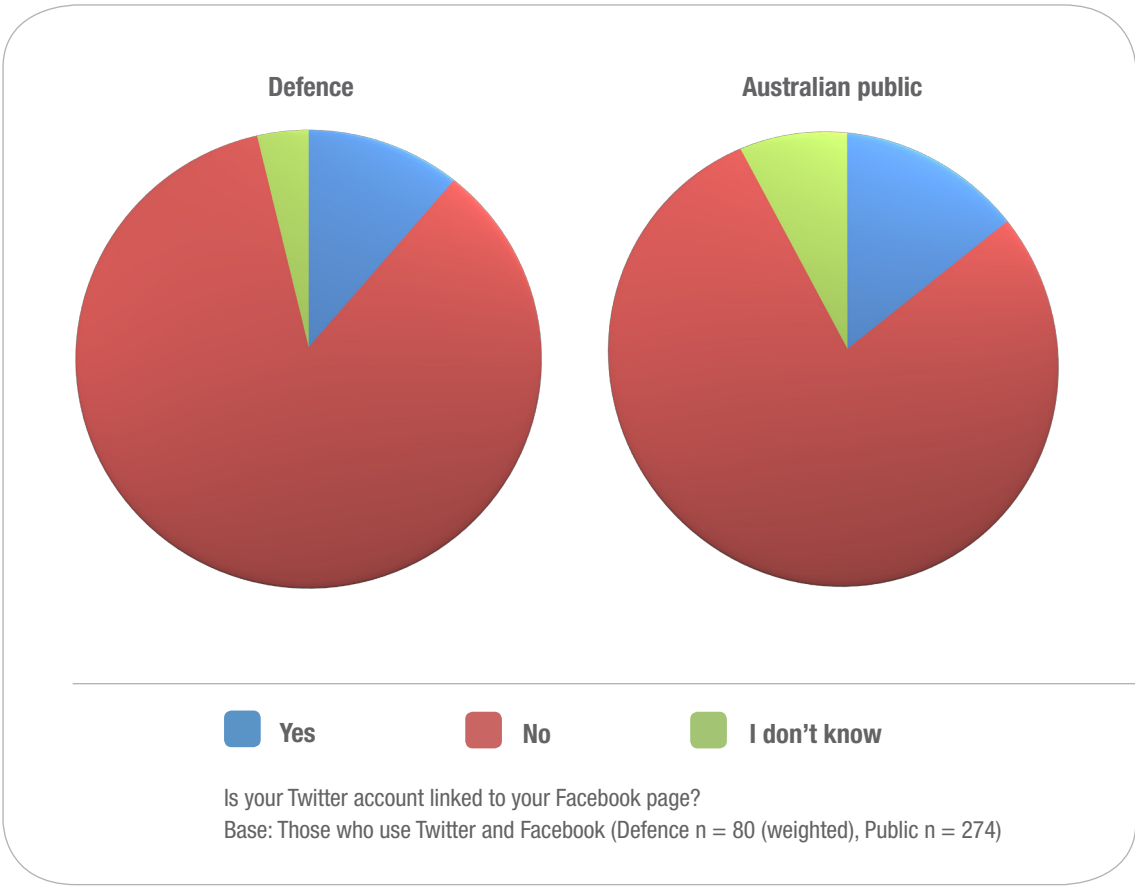
What things do you tweet about?

Base: Those who use Twitter (Defence n = 87 (weighted), Public n = 289)

	Defence	Public
Work events	11%	36%
Personal life	40%	48%
Hobbies	40%	39%
Industry info	11%	19%
Other	41%	21%

Only 11% of Defence employees tweet about work events and activities, compared to over a third of the general public.

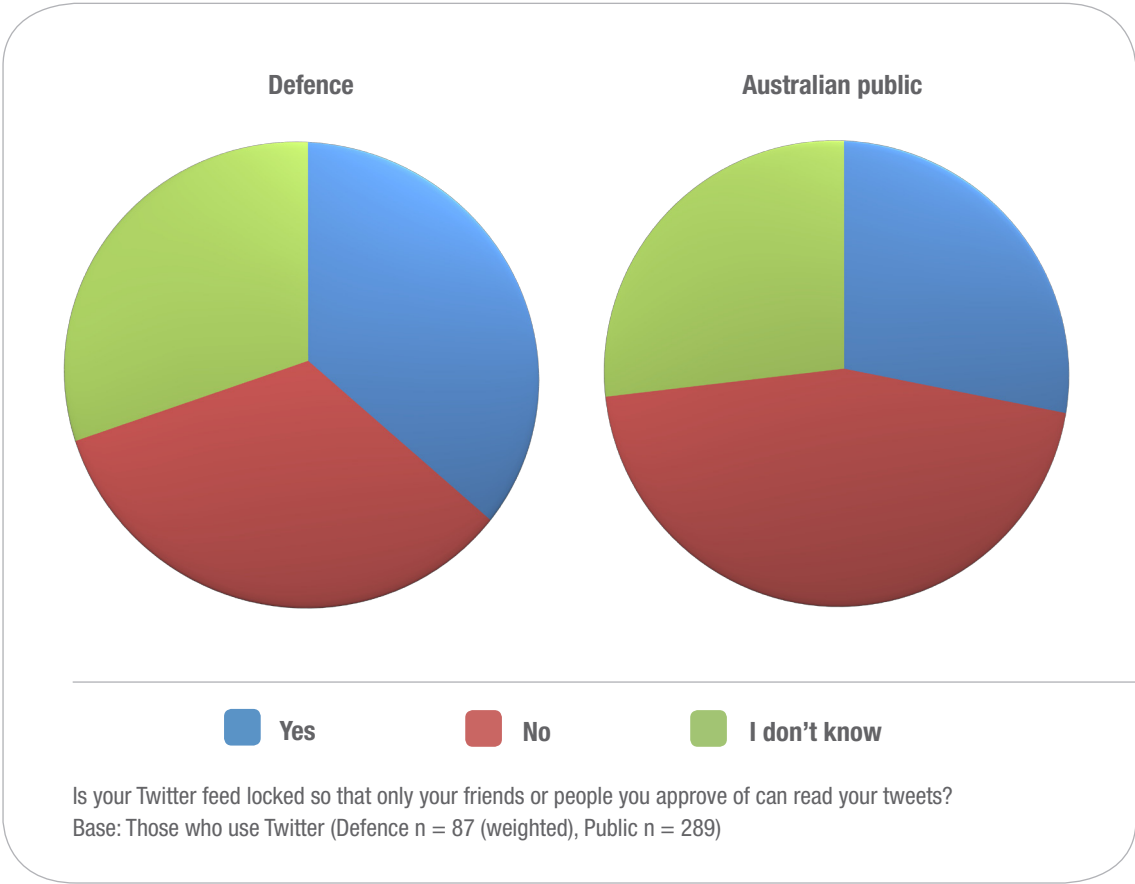
IS YOUR TWITTER ACCOUNT LINKED TO YOUR FACEBOOK PAGE?



	Defence	Public
Yes	11%	14%
No	85%	78%
I don't know	4%	8%

The vast majority of respondents (both Defence employees and the Australian public), have not linked their Twitter account to their Facebook page.

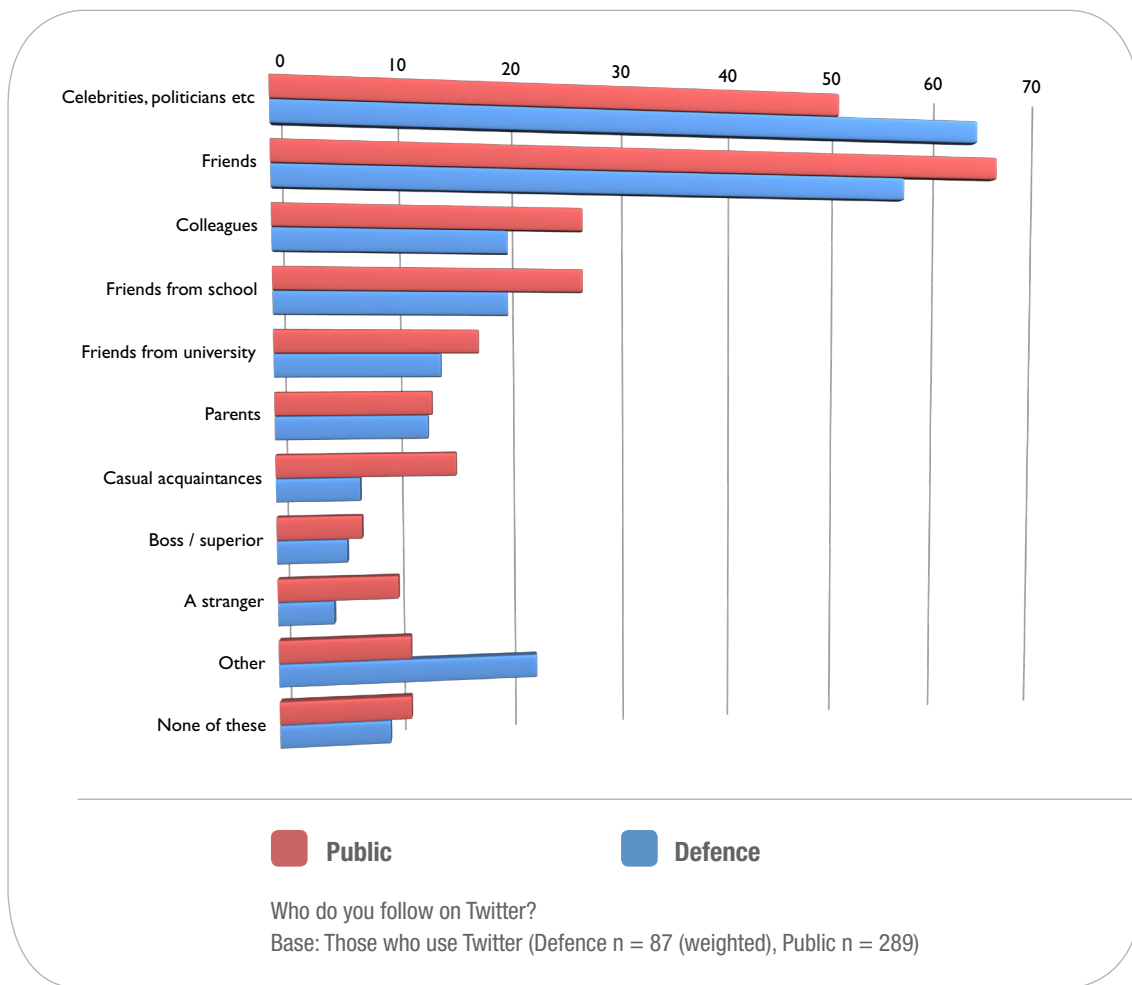
IS YOUR TWITTER FEED LOCKED?



	Defence	Public
Yes	37%	28%
No	33%	45%
I don't know	31%	27%

Defence employees are more likely to lock their Twitter feed than the Australian public, although around a third of them are unsure as to whether it is locked or not.

WHO DO YOU FOLLOW ON TWITTER?

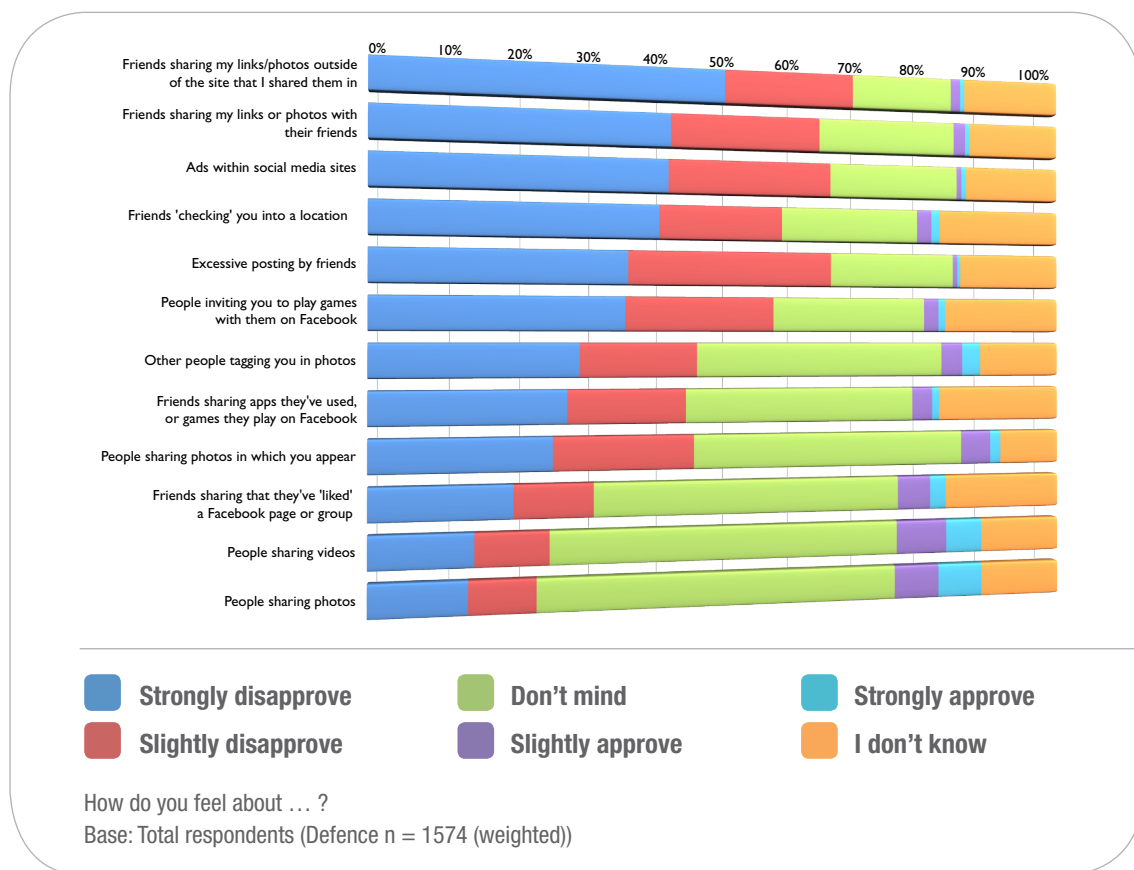


	Defence	Public
None of these	9%	11%
Other	22%	11%
A stranger	5%	10%
Boss / superior	6%	7%
Casual acquaintances	7%	15%
Parents	13%	13%
Friends from university	14%	17%
Friends from school	20%	26%
Colleagues	20%	26%
Friends	55%	64%
Celebrities, politicians etc	62%	49%

Almost two-thirds of Defence employees choose to follow celebrities, compared to just 49% of the general public, who are more likely to follow their friends.

The Australian public are more inclined than Defence employees to follow friends from school or university and casual acquaintances.

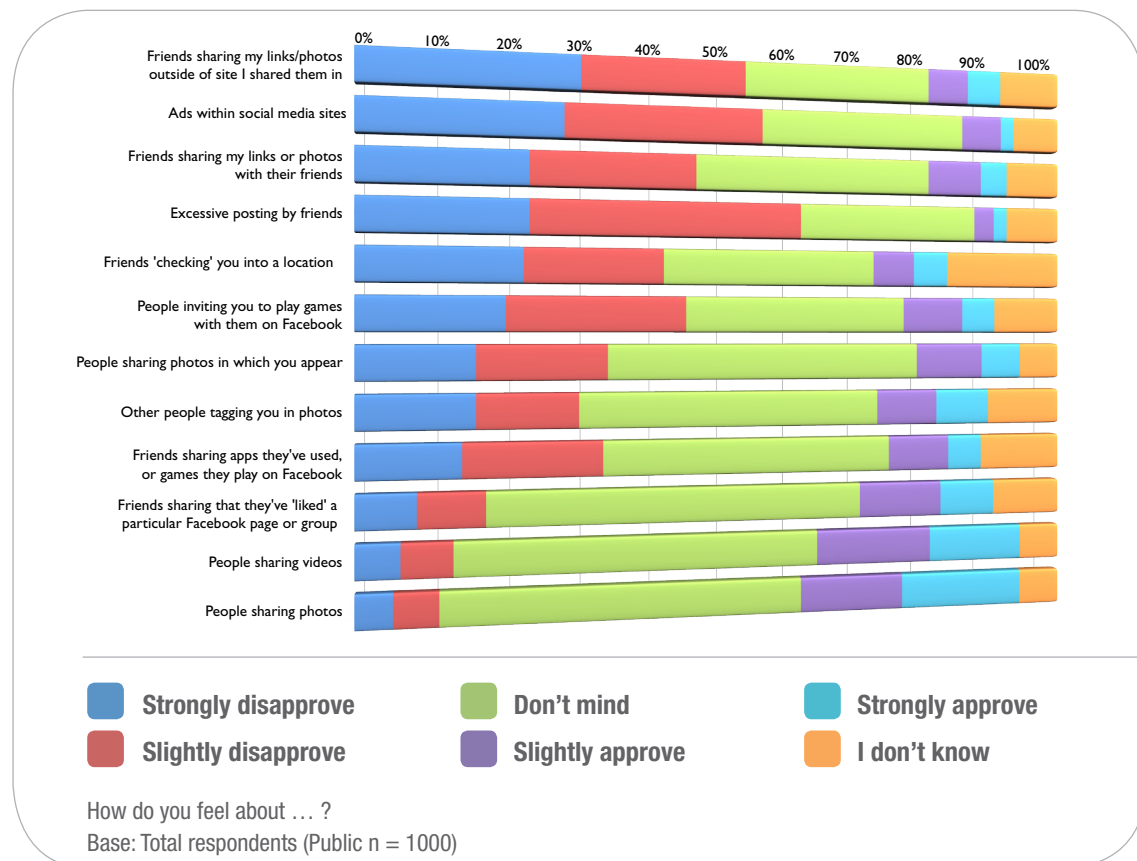
LIKES & DISLIKES – DEFENCE



	Strongly disapprove	Slightly disapprove	Don't mind	Slightly approve	Strongly approve	I don't know
People sharing photos	13%	9%	52%	7%	7%	12%
People sharing videos	14%	10%	50%	8%	5%	12%
Friends sharing that they've 'liked' a Facebook page or group	20%	11%	44%	5%	2%	18%
People sharing photos in which you appear	25%	20%	40%	5%	2%	9%
Friends sharing apps they've used, or games they play on Facebook	27%	17%	34%	3%	1%	19%
Other people tagging you in photos	29%	17%	37%	3%	3%	12%
People inviting you to play games with them on Facebook	35%	21%	23%	2%	1%	18%
Excessive posting by friends	35%	29%	19%	1%	0%	15%
Friends 'checking' you into a location	40%	18%	20%	2%	1%	19%
Ads within social media sites	41%	24%	19%	1%	1%	14%
Friends sharing my links or photos with their friends	41%	22%	21%	2%	1%	14%
Friends sharing my links/photos outside of the site that I shared them in	49%	19%	15%	1%	1%	15%

The biggest social media 'offence' is friends sharing links or photos that the respondent posted. Over two-thirds of Defence employees disapprove of this activity. Around the same number disapprove of ads within social media sites. Strongest approval was given to people sharing videos and photos.

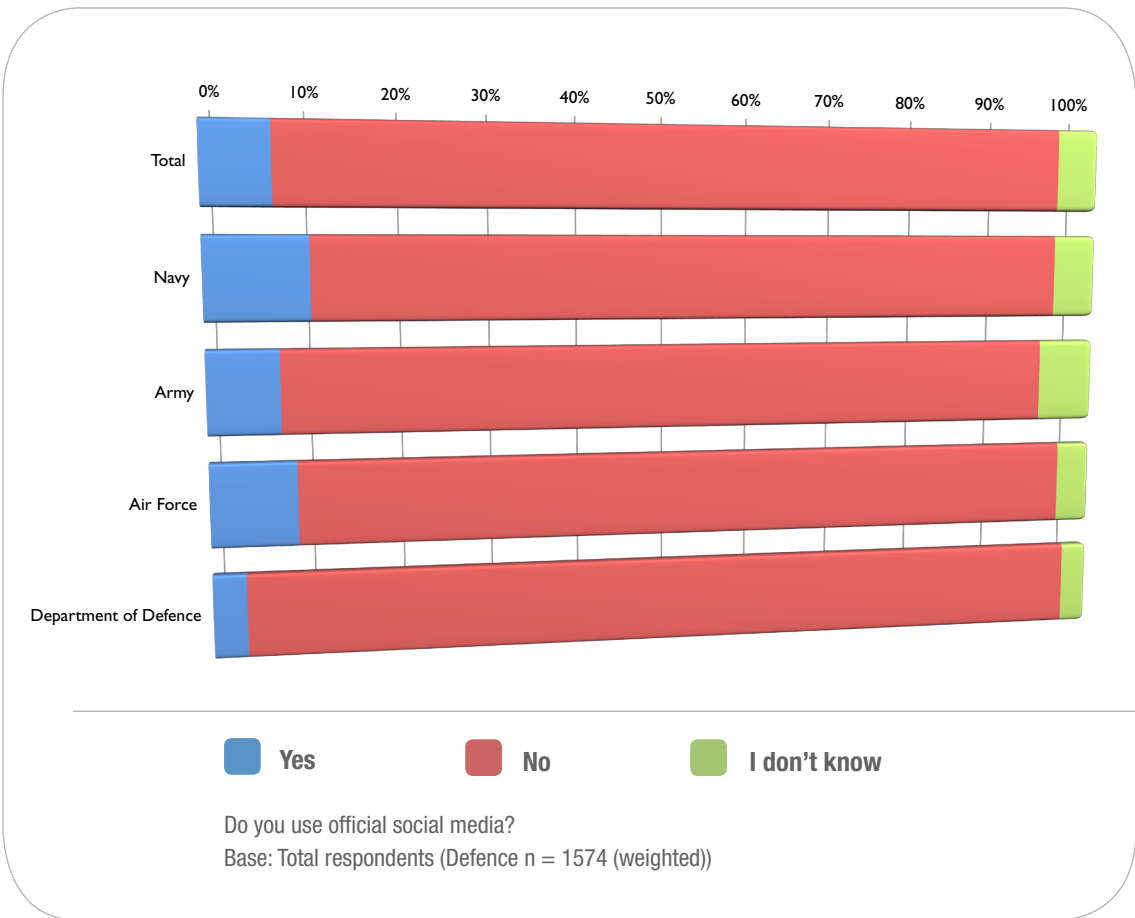
LIKES & DISLIKES – AUSTRALIAN PUBLIC



	Strongly disapprove	Slightly disapprove	Don't mind	Slightly approve	Strongly approve	I don't know
People sharing photos	5%	6%	50%	15%	18%	6%
People sharing videos	6%	7%	51%	17%	14%	6%
Friends sharing that they've 'liked' a particular Facebook page or group	8%	9%	52%	12%	8%	10%
Friends sharing apps they've used, or games they play on Facebook	14%	19%	41%	9%	5%	12%
Other people tagging you in photos	16%	14%	43%	9%	8%	11%
People sharing photos in which you appear	16%	18%	45%	10%	6%	6%
People inviting you to play games with them on Facebook	20%	25%	32%	9%	5%	10%
Friends 'checking' you into a location	22%	19%	30%	6%	5%	17%
Excessive posting by friends	23%	38%	26%	3%	2%	8%
Friends sharing my links or photos with their friends	23%	23%	34%	8%	4%	8%
Ads within social media sites	28%	28%	30%	6%	2%	7%
Friends sharing my links/photos outside of site I shared them in	30%	23%	27%	6%	5%	9%

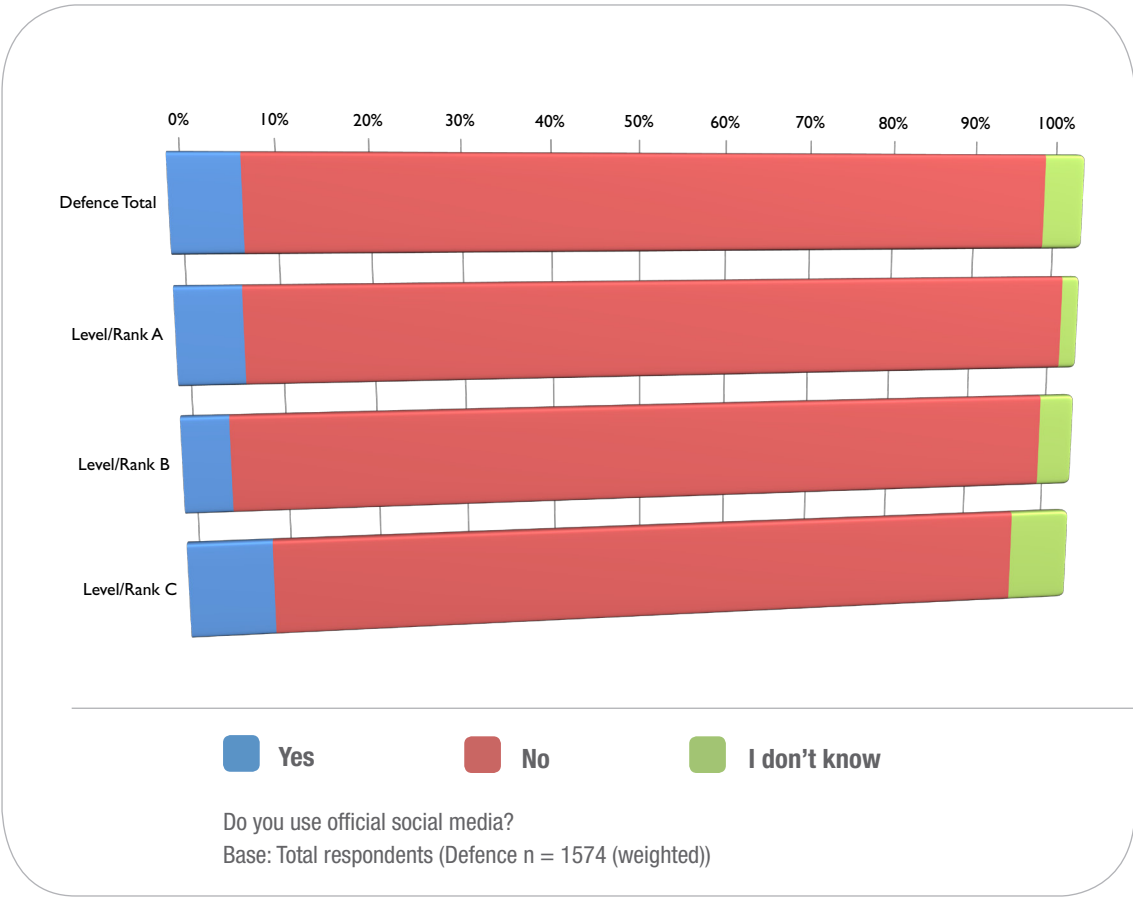
The Australian public is significantly less disapproving of social media activity than those in Defence. Friends sharing links and photos is still the biggest offence, but only 53% of Australians disapprove compared to 68% of Defence employees. At the other end of the scale, more than twice as many Australians approve of people sharing videos or photos than do those in Defence.

DO YOU USE OFFICIAL SOCIAL MEDIA? (BY EMPLOYMENT SERVICE)



	Defence Total	Navy	Army	Air Force	Department of Defence
Yes	7%	11%	8%	9%	4%
No	88%	84%	86%	87%	94%
I don't know	5%	5%	6%	4%	3%

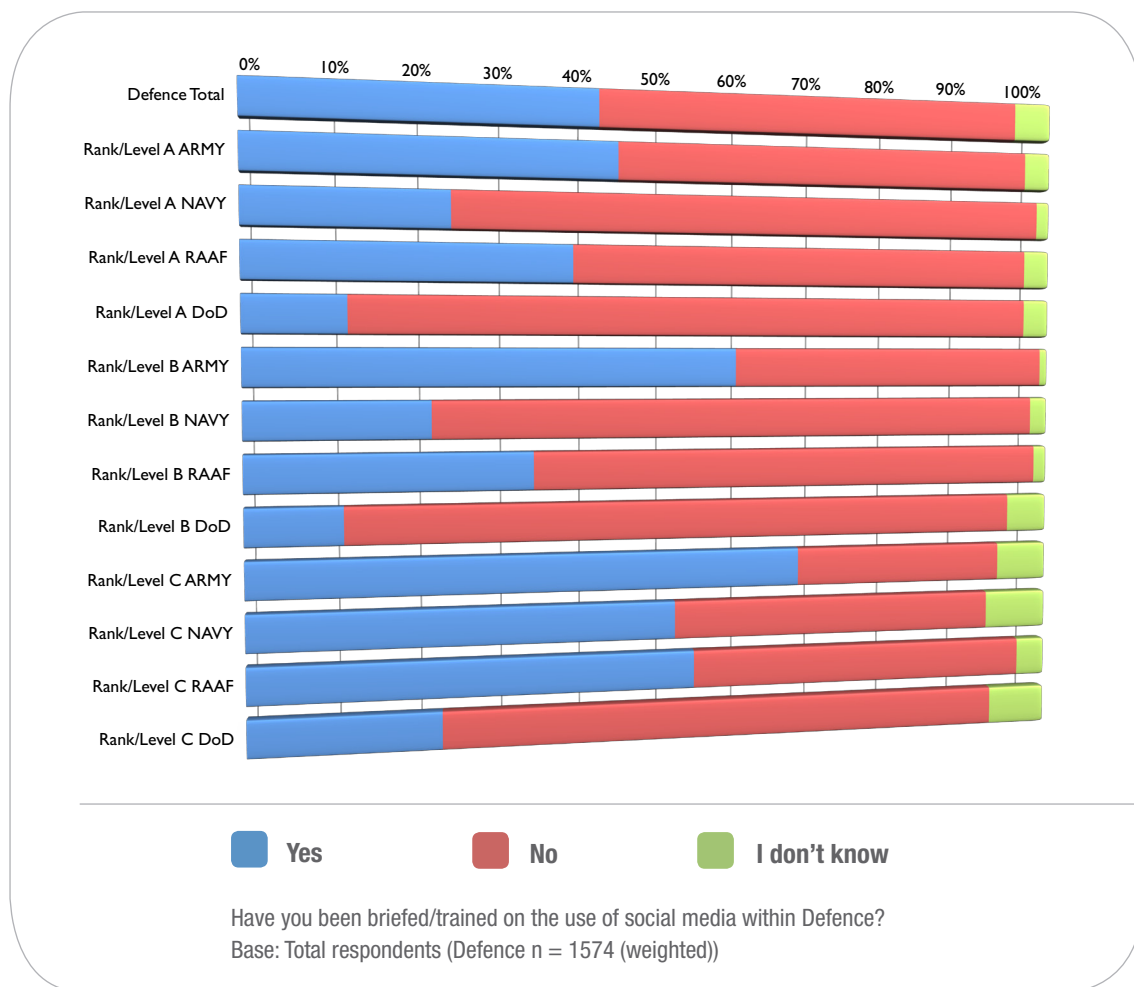
DO YOU USE OFFICIAL SOCIAL MEDIA? (BY LEVEL/RANK)



	Defence Total	Level/ Rank A	Level/ Rank B	Level/ Rank C
Yes	7%	7%	5%	9%
No	88%	92%	91%	85%
I don't know	5%	2%	4%	7%

The vast majority of Defence personnel do not use official social media. Usage is slightly higher among those at Rank/Level C, particularly those employed by the Navy.

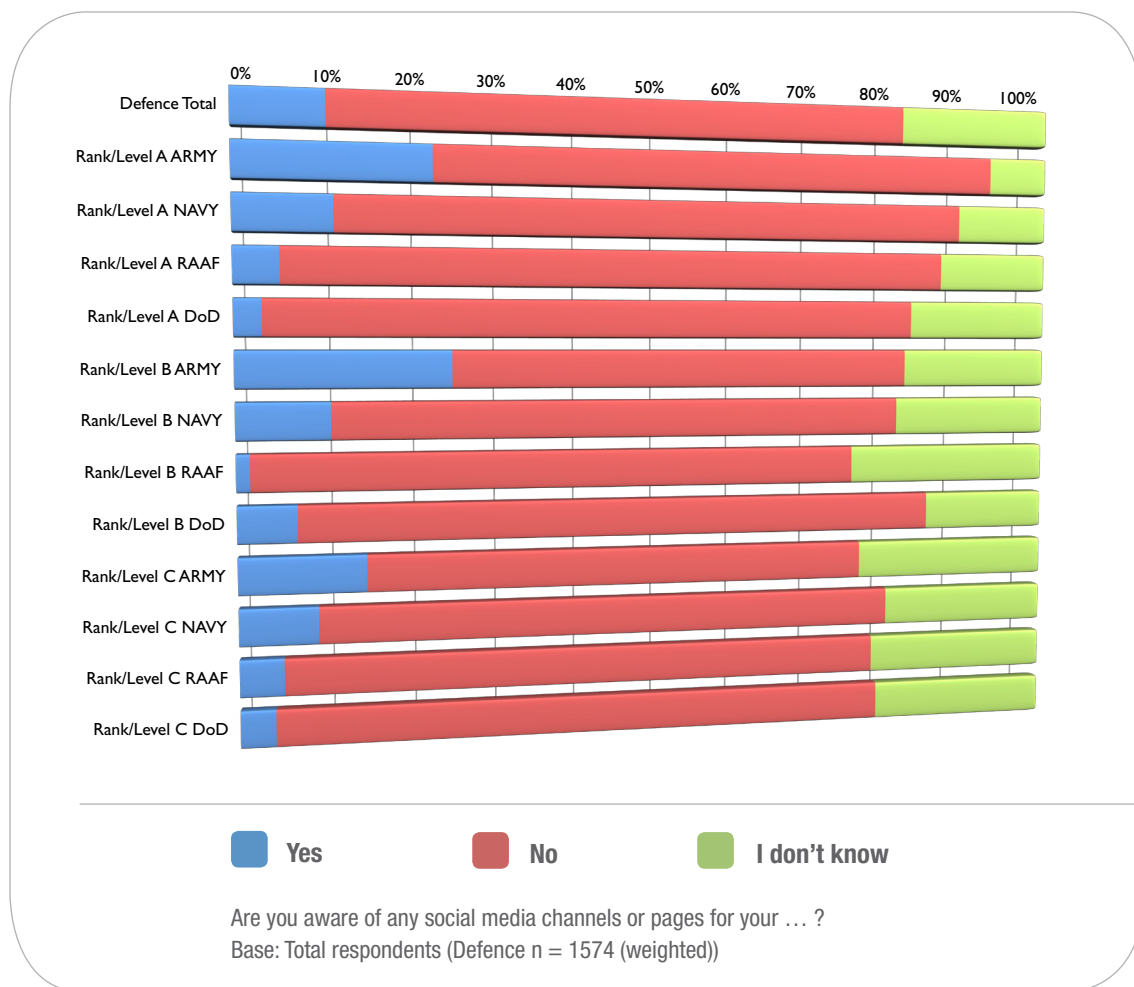
HAVE YOU BEEN TRAINED/BRIEFED ON THE USE OF SOCIAL MEDIA?



	Defence Total	A Army	A NAVY	A RAAF	A DoD	B Army	B Navy	B RAAF	B DoD	C ARMY	C NAVY	C RAAF	C DoD
Yes	42%	44%	25%	38%	12%	58%	22%	34%	11%	67%	51%	54%	23%
No	53%	52%	75%	57%	85%	40%	76%	65%	83%	27%	41%	43%	70%
I don't know	5%	3%	2%	3%	3%	1%	2%	2%	5%	6%	8%	4%	7%

Overall, 42% of Defence employees have been trained on the use of social media. Army personnel are more likely to have been trained than their Navy, RAAF and DoD counterparts, particularly those at Rank/Level C, of whom two-thirds claim to have been briefed. Conversely, DoD employees are least likely to have been trained, particularly those at Level/Rank A or B.

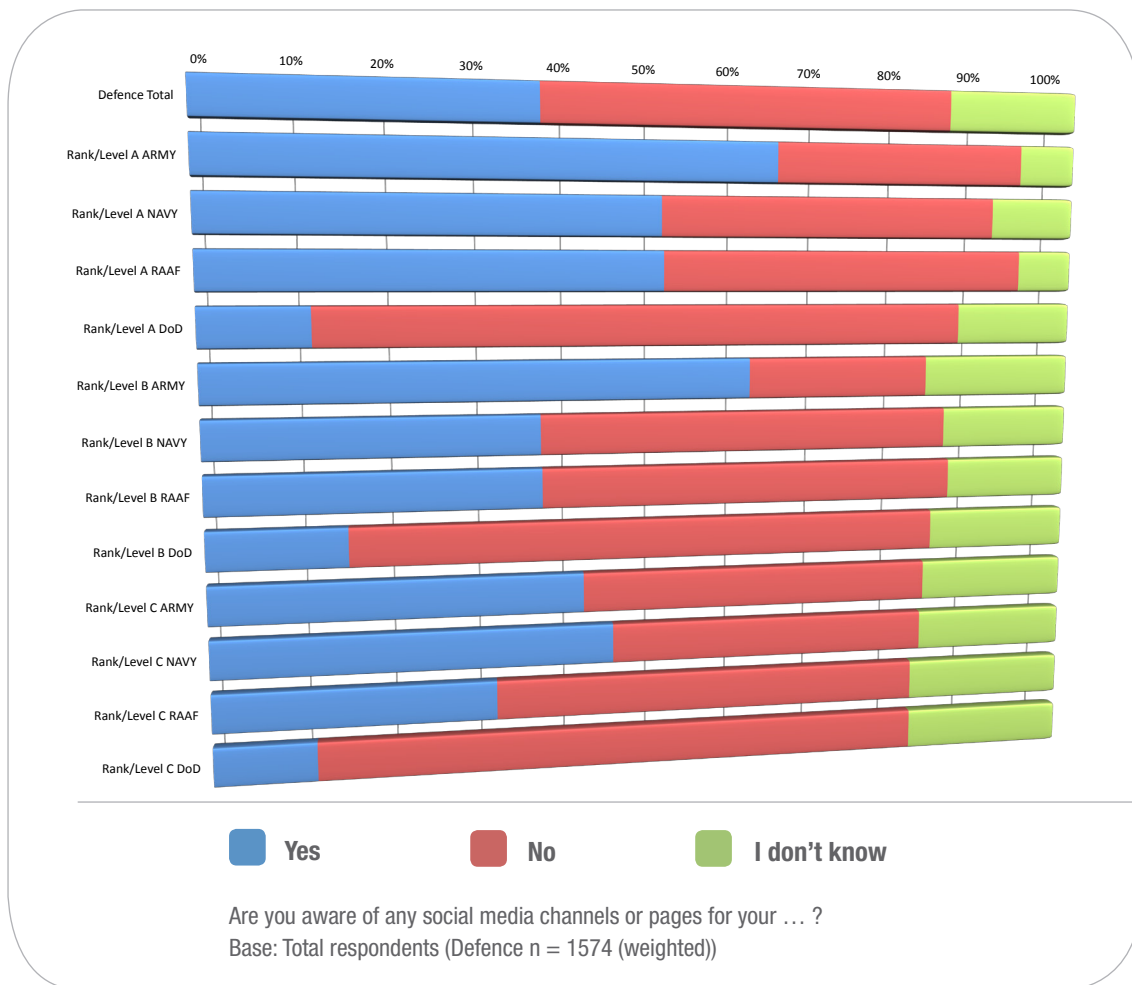
ARE YOU AWARE OF ANY SOCIAL MEDIA CHANNELS/PAGES FOR YOUR REGIMENT?



	Defence Total	A Army	A NAVY	A RAAF	A DoD	B Army	B Navy	B RAAF	B DoD	C ARMY	C NAVY	C RAAF	C DoD
Yes	11%	23%	11%	5%	3%	25%	11%	2%	7%	15%	9%	5%	4%
No	70%	70%	77%	81%	79%	56%	70%	74%	78%	61%	70%	72%	74%
I don't know	19%	7%	11%	14%	18%	19%	20%	26%	15%	24%	21%	22%	22%

Awareness of their regiment's social media channels/pages is highest among Army personnel, particularly those at Level/Rank A and B. Around a quarter of respondents within these groups claimed awareness, compared to just 3% and 7%, respectively, for their DoD counterparts.

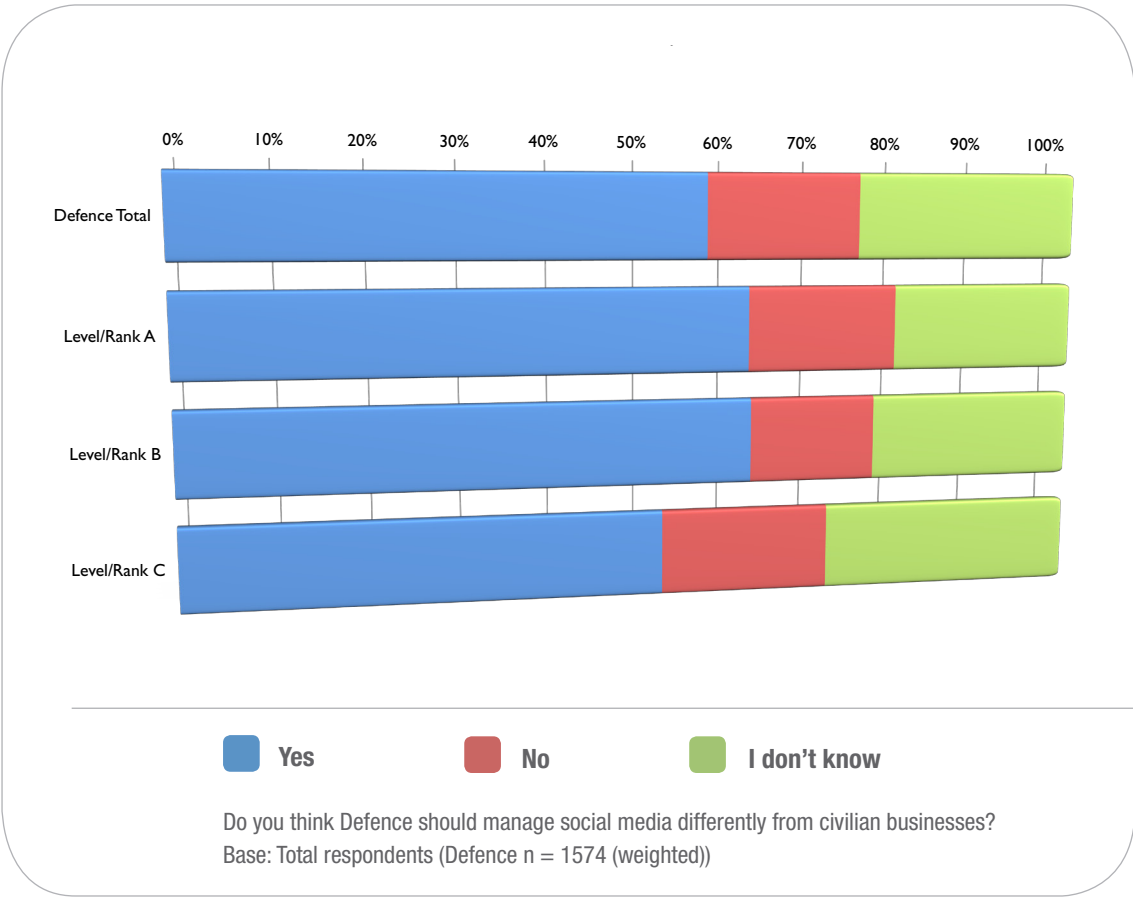
ARE YOU AWARE OF ANY SOCIAL MEDIA CHANNELS/PAGES FOR YOUR EMPLOYER?



	Defence Total	A Army	A NAVY	A RAAF	A DoD	B Army	B Navy	B RAAF	B DoD	C ARMY	C NAVY	C RAAF	C DoD
Yes	37%	65%	51%	51%	12%	61%	37%	37%	15%	42%	45%	32%	11%
No	47%	30%	39%	43%	74%	21%	48%	48%	68%	41%	37%	50%	70%
I don't know	15%	7%	10%	6%	14%	18%	15%	15%	17%	17%	18%	19%	19%

Awareness of employers' channels and pages is highest among Army groups A and B respondents, of whom over 60% of respondents indicate that they are aware. Around half of all Navy and RAAF personnel at Level/Rank A also claim awareness – a considerably higher proportion than among their Rank/Level B and C colleagues. DoD employees have the lowest awareness.

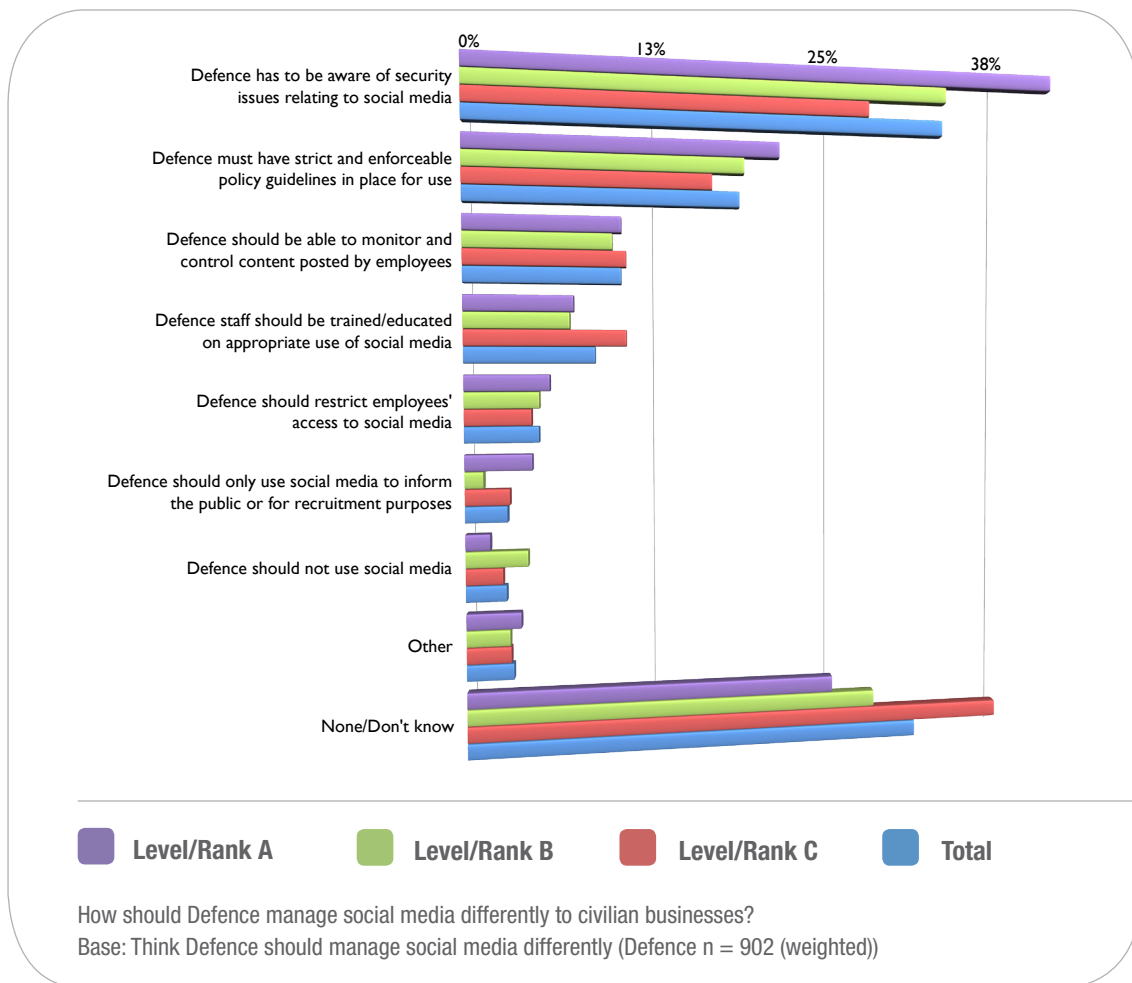
DO YOU THINK DEFENCE SHOULD MANAGE SOCIAL MEDIA DIFFERENTLY FROM CIVILIAN BUSINESSES?



	Defence Total	Level/Rank A	Level/Rank B	Level/Rank C
Yes	57%	62%	62%	52%
No	17%	17%	14%	19%
I don't know	25%	21%	23%	29%

Sixty-two per cent of Defence personnel at Level/Rank A and B believe that Defence should manage social media differently from civilian businesses. This compares to just 52% of their Level/Rank C colleagues, who are less sure on the matter.

HOW SHOULD DEFENCE MANAGE SOCIAL MEDIA DIFFERENTLY?



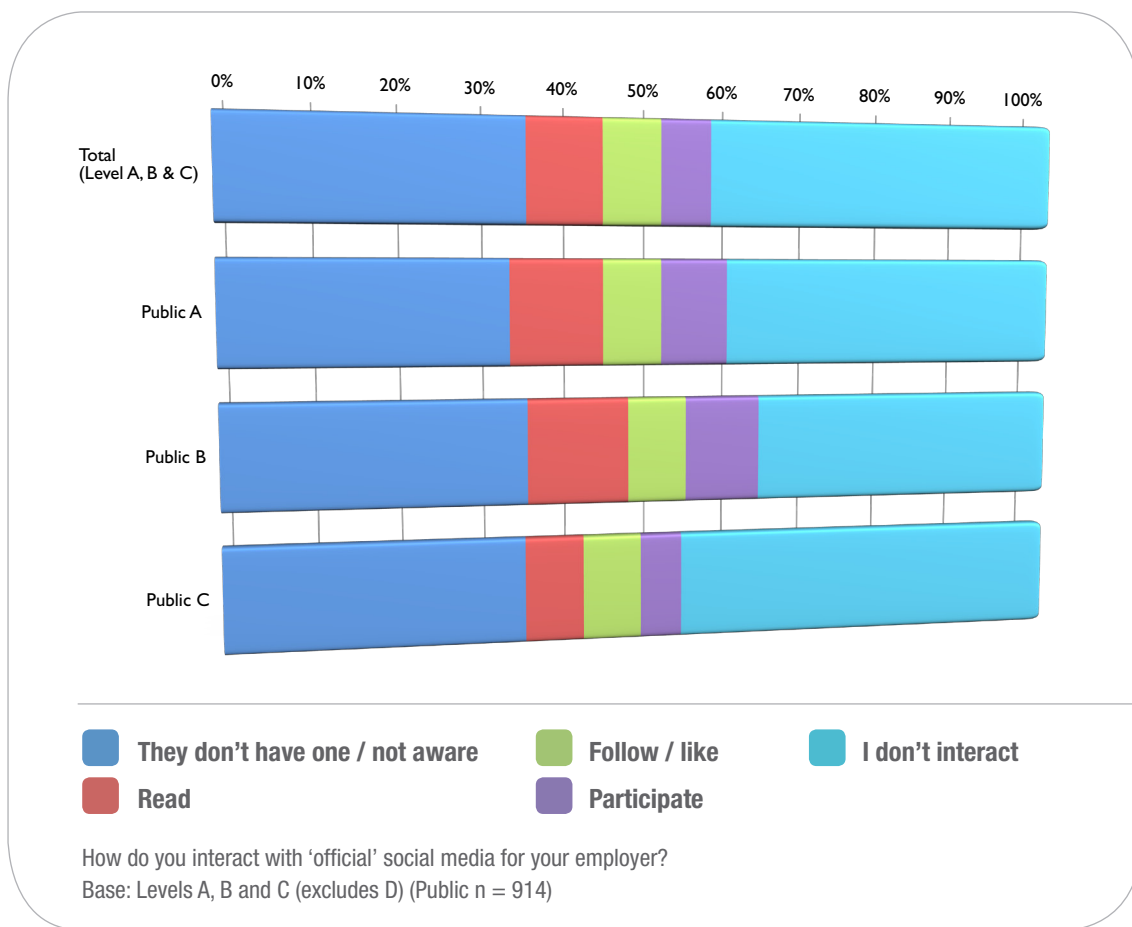
	Total	Level/ Rank A	Level/ Rank B	Level/ Rank C
None/Don't know	31%	25%	28%	37%
Other	3%	4%	3%	3%
Defence should not use social media	3%	2%	4%	2%
Defence should only use social media to inform the public or for recruitment purposes	3%	4%	1%	3%
Defence should restrict employees' access to social media	5%	6%	5%	4%
Defence staff should be trained/educated on appropriate use of social media	9%	7%	7%	11%
Defence should be able to monitor and control content posted by employees	10%	10%	10%	11%
Defence must have strict and enforceable policy guidelines in place for use	19%	21%	19%	17%
Defence has to be aware of security issues relating to social media	33%	41%	33%	28%

Employees believe that Defence needs to be aware of security issues in social media, particularly those at Level/Rank A.

Respondents also feel that there need to be strict policy guidelines in place for social media.

Around one in 10 employees thinks that Defence should be able to monitor and control social media content posted by employees.

HOW DO YOU INTERACT WITH 'OFFICIAL' SOCIAL MEDIA FOR YOUR EMPLOYER?

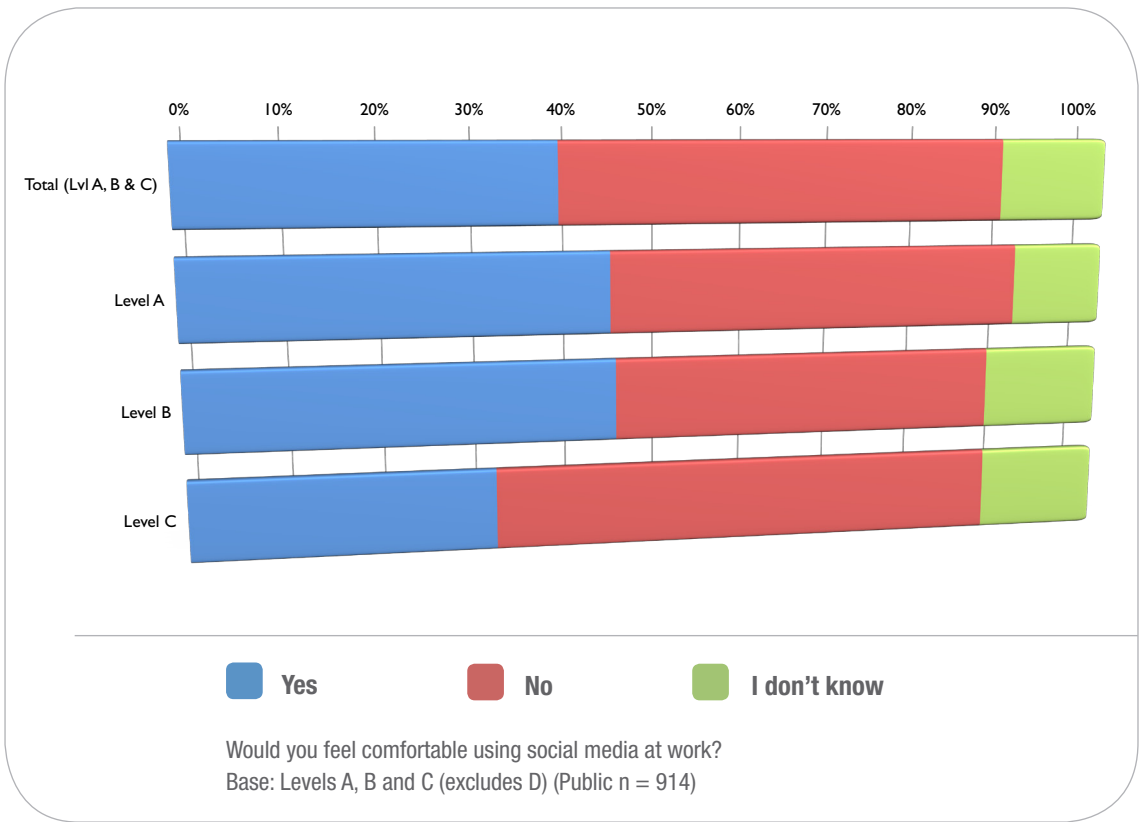


	Total (Lvl A, B & C)	Public A	Public B	Public C
They don't have one / not aware	35%	33%	35%	35%
Read	9%	11%	12%	7%
Follow / like	7%	7%	7%	7%
Participate	6%	8%	9%	5%
I don't interact	43%	41%	37%	47%

The majority of Australians either are not aware of their employer's official social media or else they do not interact with it.

Twenty-two per cent of respondents claim to either read, follow or participate in their employer's social media channel/page. This rises to 28% among Level B respondents.

WOULD YOU FEEL COMFORTABLE USING SOCIAL MEDIA AT WORK?

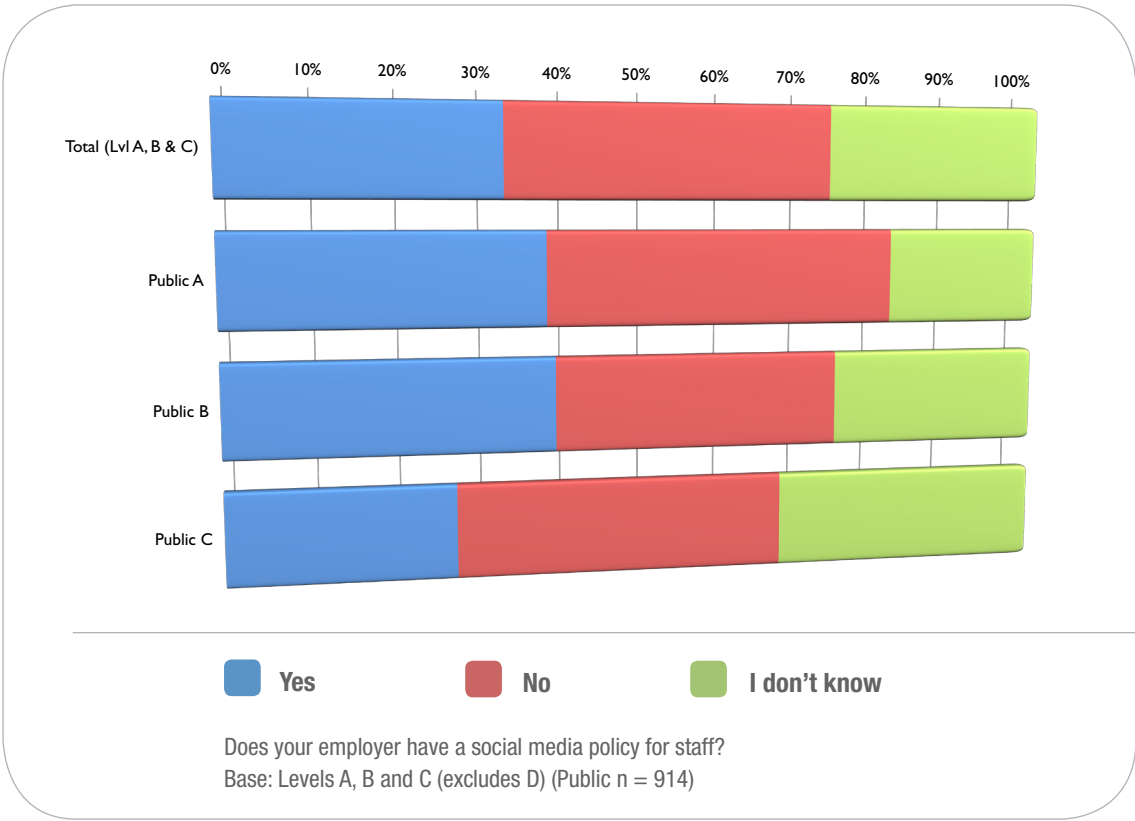


	Total (Lvl A, B & C)	Public A	Public B	Public C
Yes	39%	44%	45%	32%
No	49%	45%	42%	55%
I don't know	12%	10%	13%	13%

Overall, 39% of Australians agreed that they would feel comfortable using social media at work.

Level C respondents were the least likely to be comfortable with it.

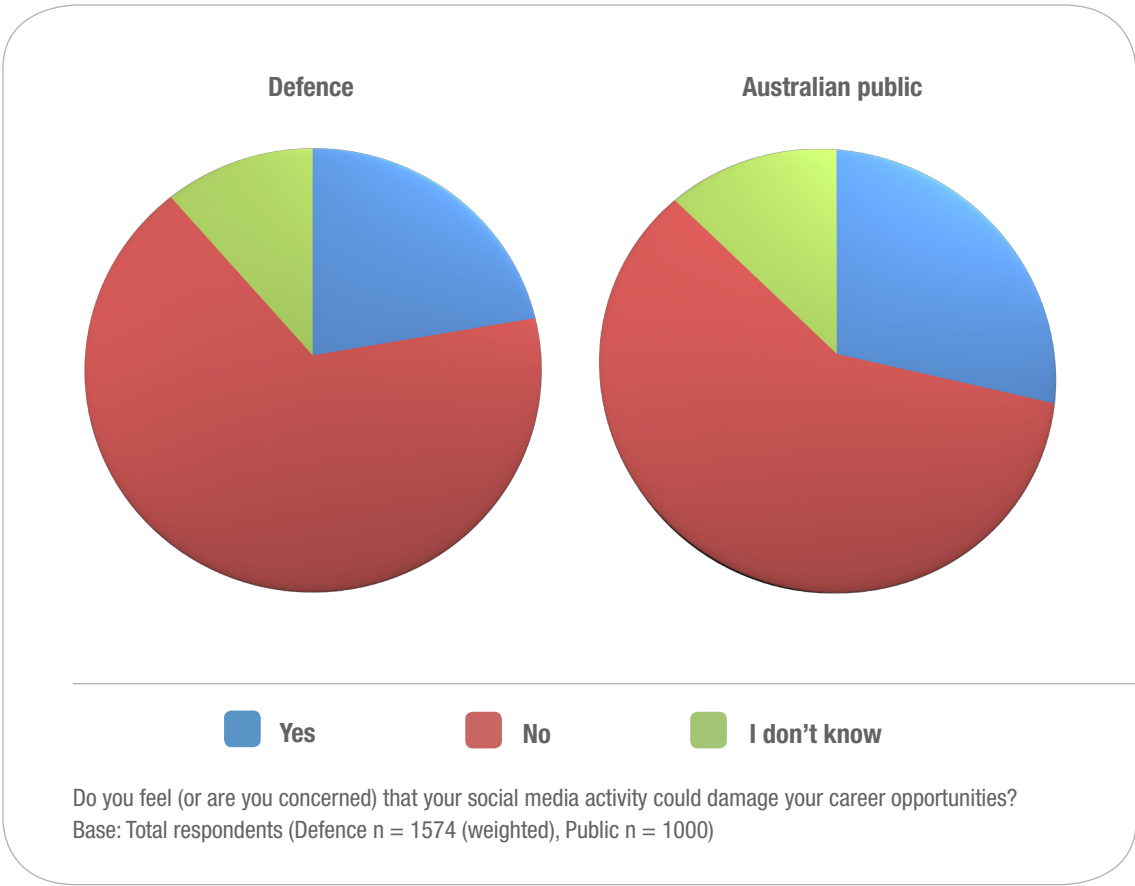
DOES YOUR EMPLOYER HAVE A SOCIAL MEDIA POLICY FOR STAFF?



	Total (Lvl A, B & C)	Public A	Public B	Public C
Yes	33%	38%	39%	27%
No	40%	43%	35%	40%
I don't know	27%	19%	26%	33%

Almost 40% of respondents from Levels A and B indicated that their employers have a social media policy. This drops to just 27% for Level C respondents.

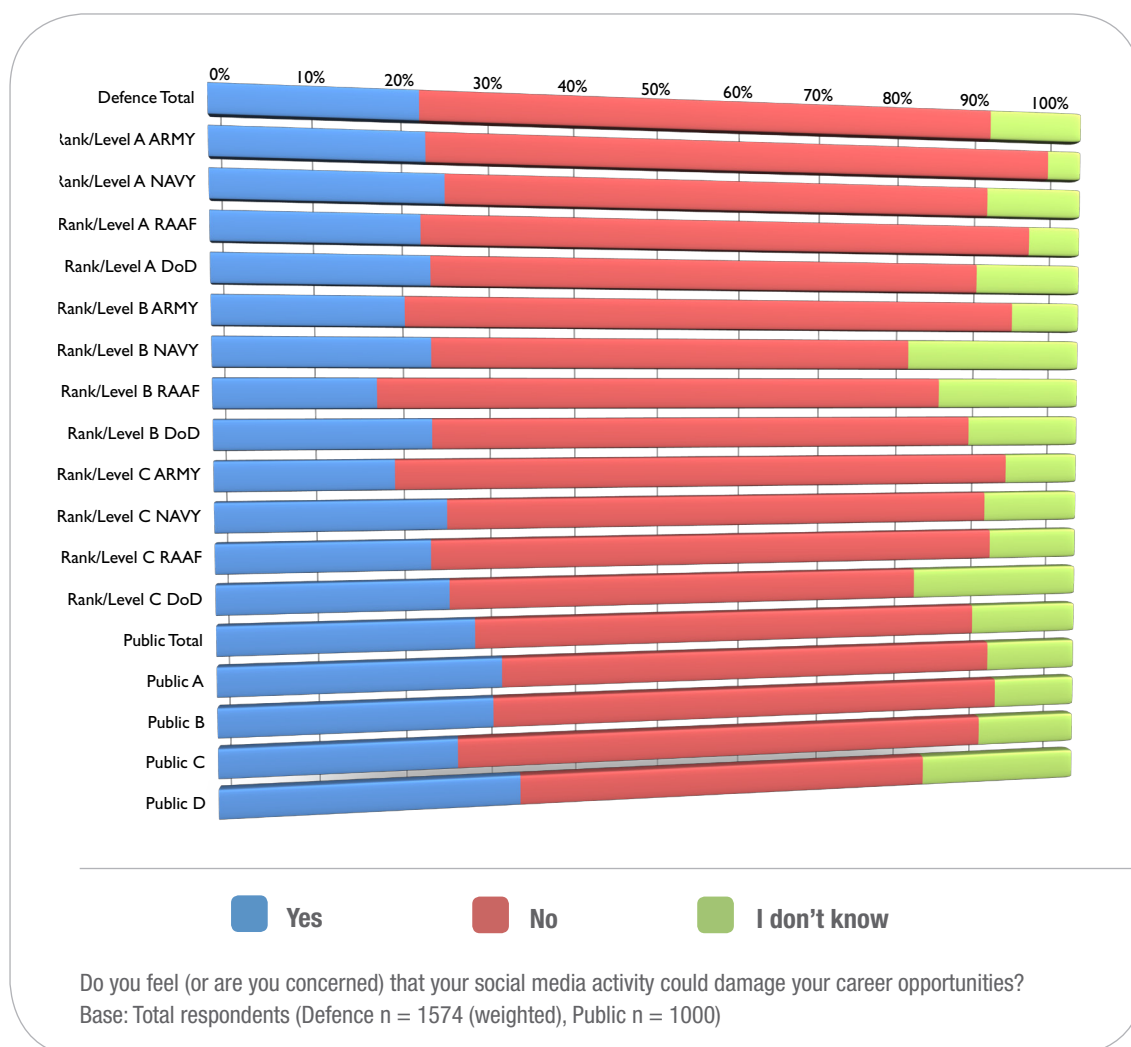
DO YOU FEEL YOUR SOCIAL MEDIA ACTIVITY COULD DAMAGE YOUR CAREER OPPORTUNITIES?



	Defence	Public
Yes	22%	28%
No	66%	59%
I don't know	11%	13%

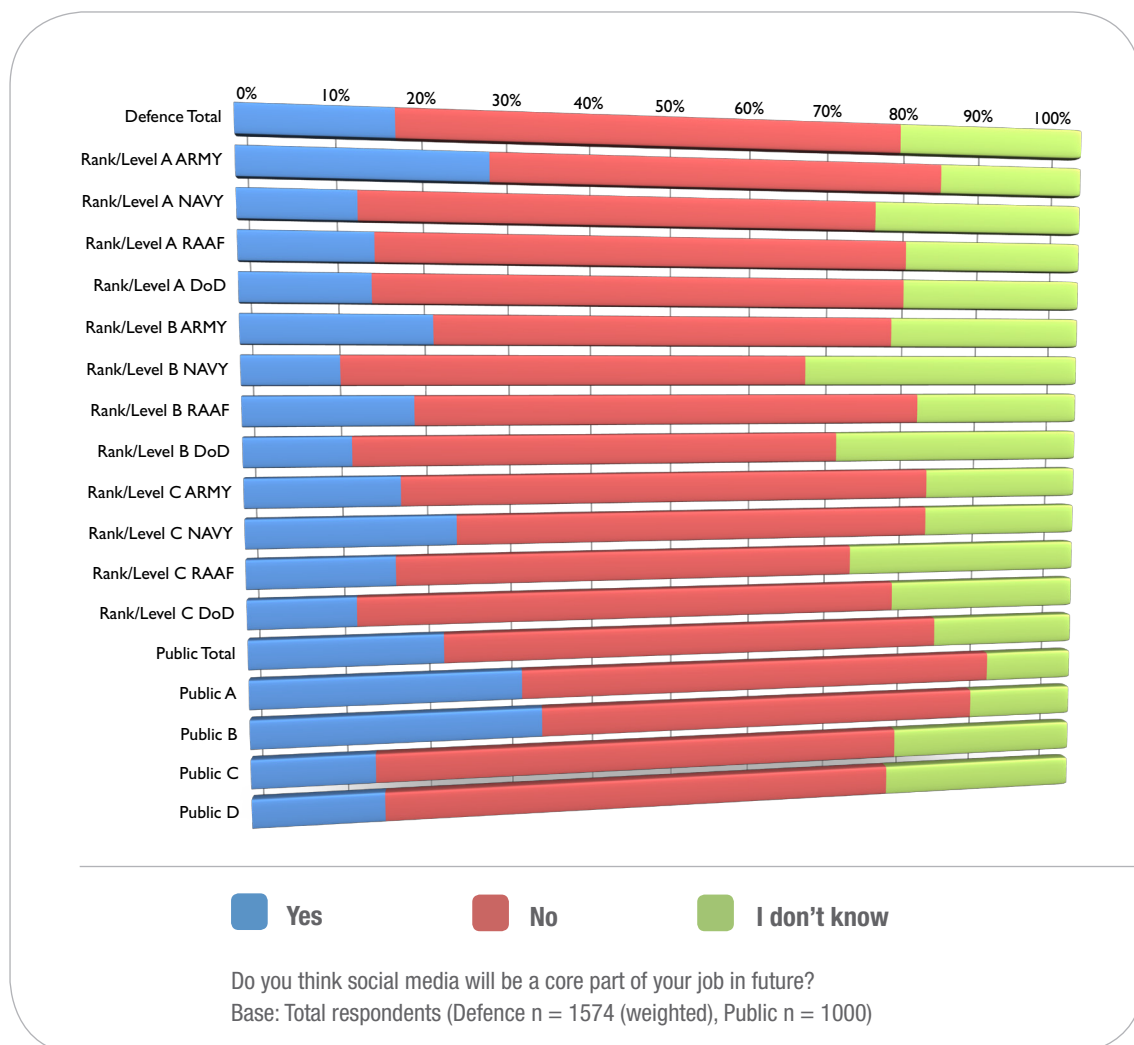
Compared to Defence employees, the Australian public are more likely to feel that their social media activity could harm their career. This could be an indication that Defence personnel are more cautious about their social media activity and therefore are not concerned that it could be damaging.

DO YOU FEEL YOUR SOCIAL MEDIA ACTIVITY COULD DAMAGE YOUR CAREER OPPORTUNITIES?



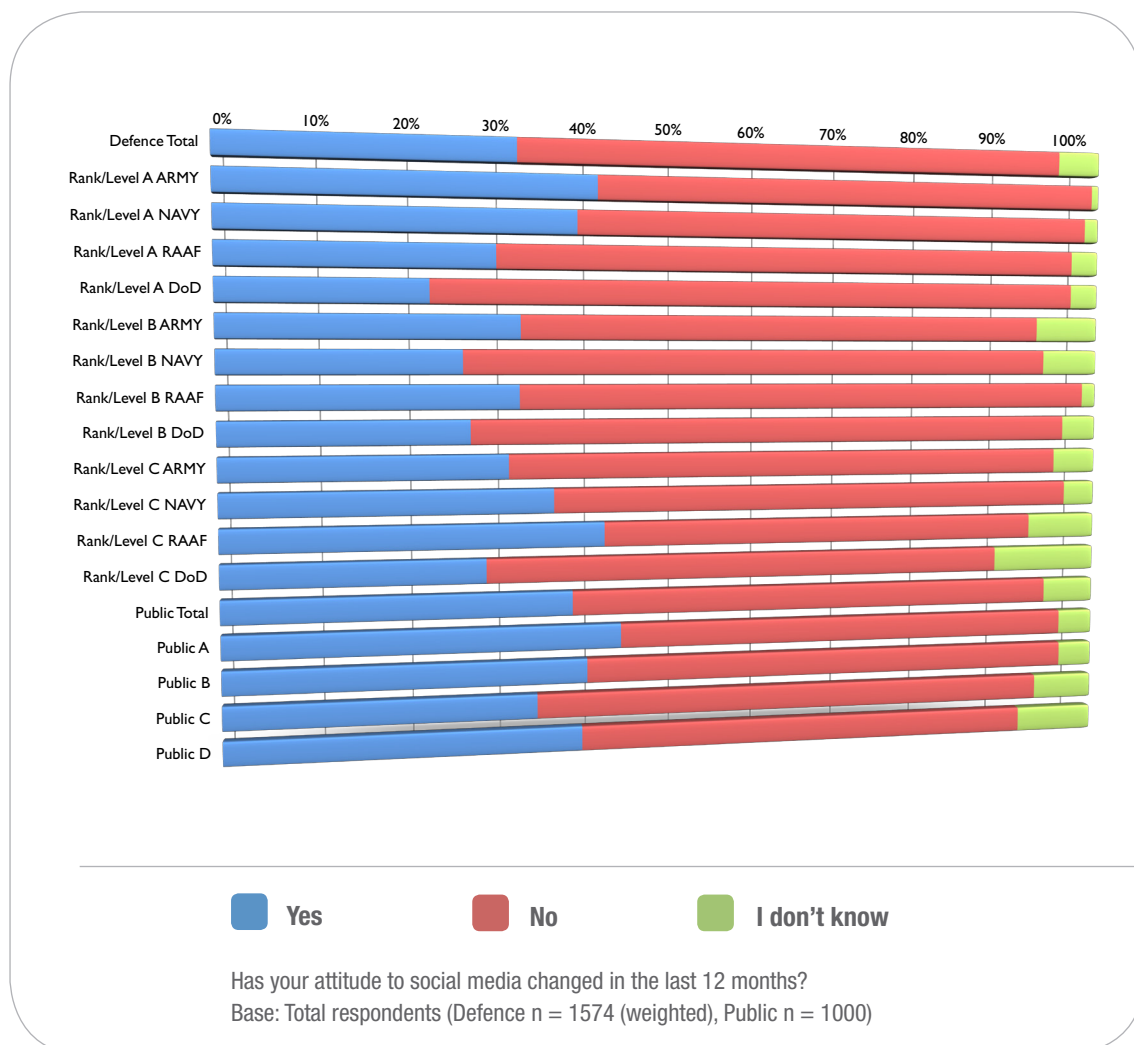
Navy personnel are slightly more likely to be concerned about their social media activity than their Army, RAAF or DoD counterparts.

DO YOU THINK SOCIAL MEDIA WILL BE A CORE PART OF YOUR JOB IN FUTURE?



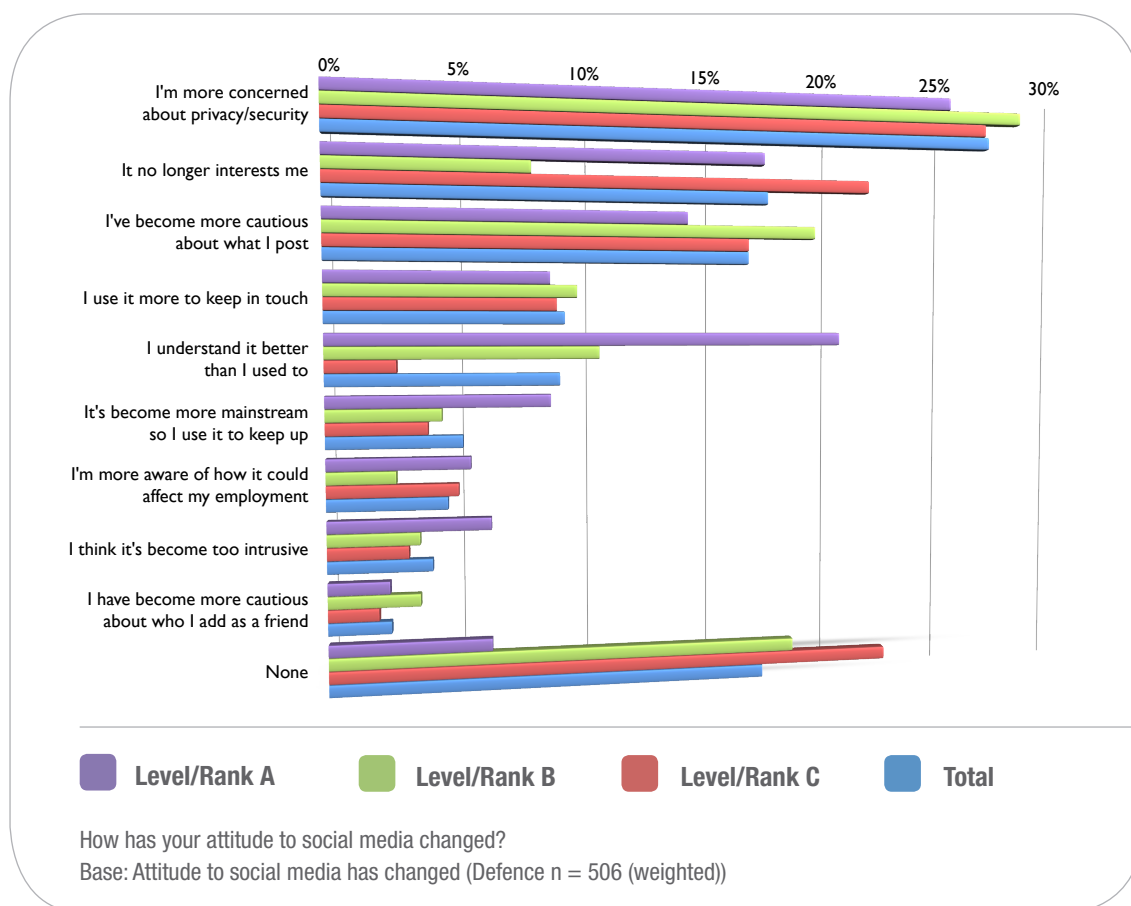
Over a quarter of Rank/Level A Army respondents believe that social media will become a core part of their job – almost twice the level reported for their Rank/Level A Navy, RAAF and DoD colleagues. Public groups A and B score higher yet; around a third of respondents expect social media to be integral to their jobs in future.

HAS YOUR ATTITUDE TO SOCIAL MEDIA CHANGED IN THE LAST 12 MONTHS?



Thirty-two per cent of Defence employees indicated that their attitude to social media has changed in the past 12 months, compared to 38% among the general public. Within Defence, both Army Rank/Level A and RAAF Rank/Level C recorded a particularly high proportion whose attitude has changed (41%); however, public Group A scored higher than either with 43%.

HOW HAS YOUR ATTITUDE TO SOCIAL MEDIA CHANGED? DEFENCE



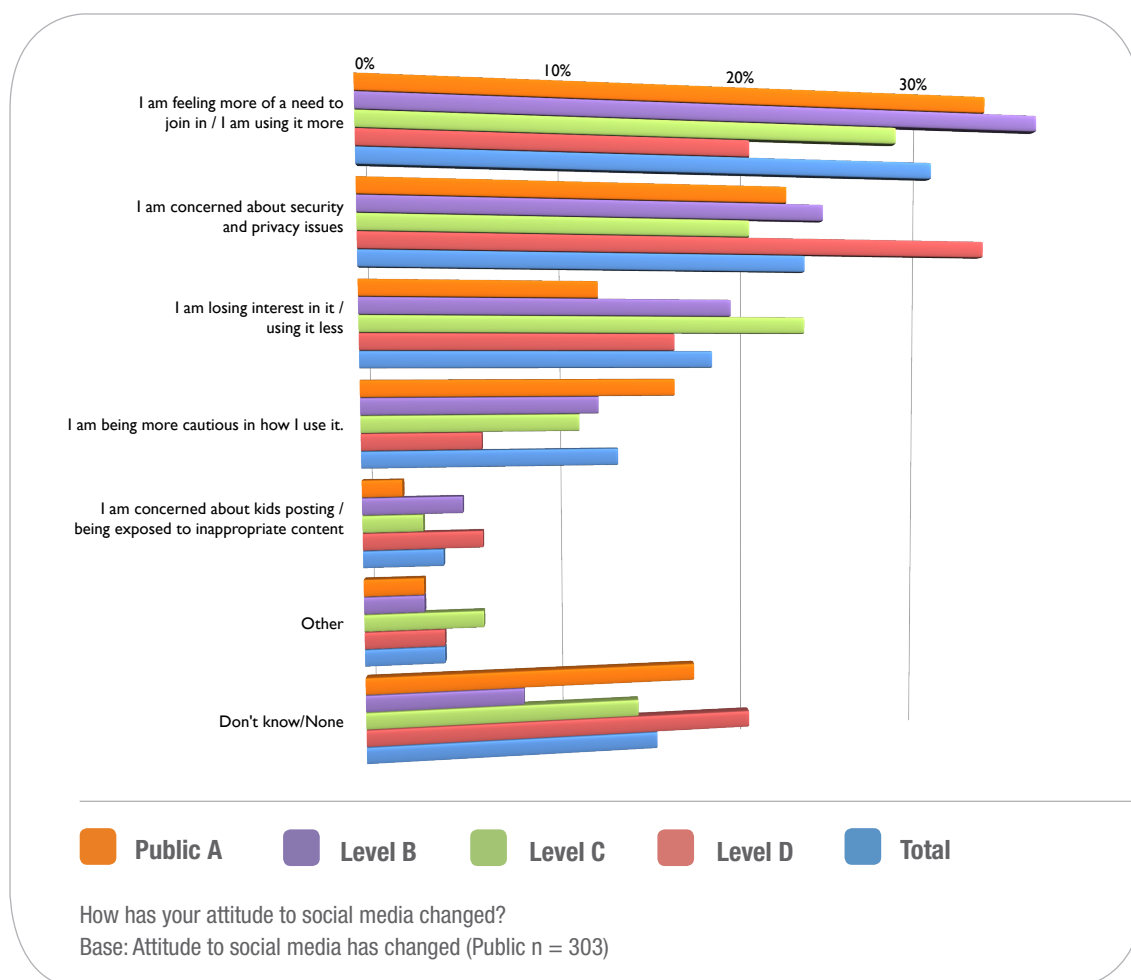
	Defence Total	Level /Rank A	Level /Rank B	Level /Rank C
None	17%	6%	18%	22%
I have become more cautious about who I add as a friend	2%	2%	3%	2%
I think it's become too intrusive	4%	6%	3%	3%
I'm more aware of how it could affect my employment	5%	5%	3%	5%
It's become more mainstream so I use it to keep up	5%	9%	4%	4%
I understand it better than I used to	9%	20%	10%	3%
I use it more to keep in touch	9%	9%	10%	9%
I've become more cautious about what I post	16%	14%	19%	16%
It no longer interests me	17%	17%	8%	21%
I'm more concerned about privacy/security	26%	25%	28%	26%

Among those Defence personnel who indicated that their attitude to social media has changed, security is the biggest issue – 26% indicated that they have become increasingly concerned about their online privacy.

Seventeen per cent claimed that social media no longer interests them. This figure increases to 21% among Level/Rank C respondents.

Around a fifth of Level/Rank A respondents commented that they understand social media more than they used to.

HOW HAS YOUR ATTITUDE TO SOCIAL MEDIA CHANGED? PUBLIC



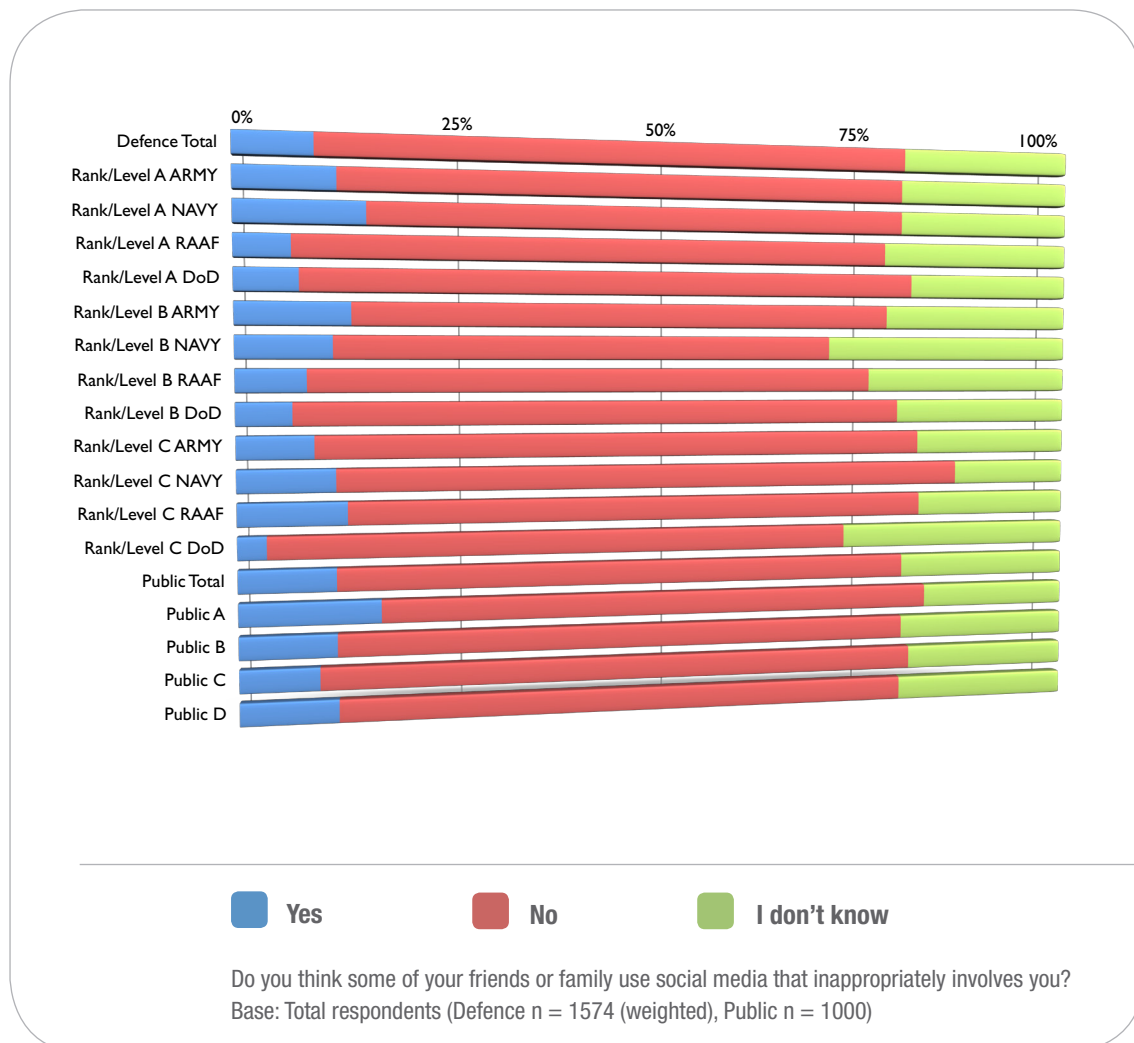
	Total	Level A	Level B	Level C	Public D
Don't know/None	15%	17%	8%	14%	20%
Other	4%	3%	3%	6%	4%
I am concerned about kids posting / being exposed to inappropriate content	4%	2%	5%	3%	6%
I am being more cautious in how I use it.	13%	16%	12%	11%	6%
I am losing interest in it / using it less	18%	12%	19%	23%	16%
I am concerned about security and privacy issues	23%	22%	24%	20%	33%
I am feeling more of a need to join in / I am using it more	30%	33%	36%	28%	20%

Thirty per cent of the general public indicated that they are using social media more than they used to.

Around a quarter of respondents suggested that they have become increasingly concerned with security and privacy issues, a similar level to that within Defence.

Eighteen per cent of Australians commented that they are losing interest in social media or are using it less than they used to, similar to the proportion among Defence employees.

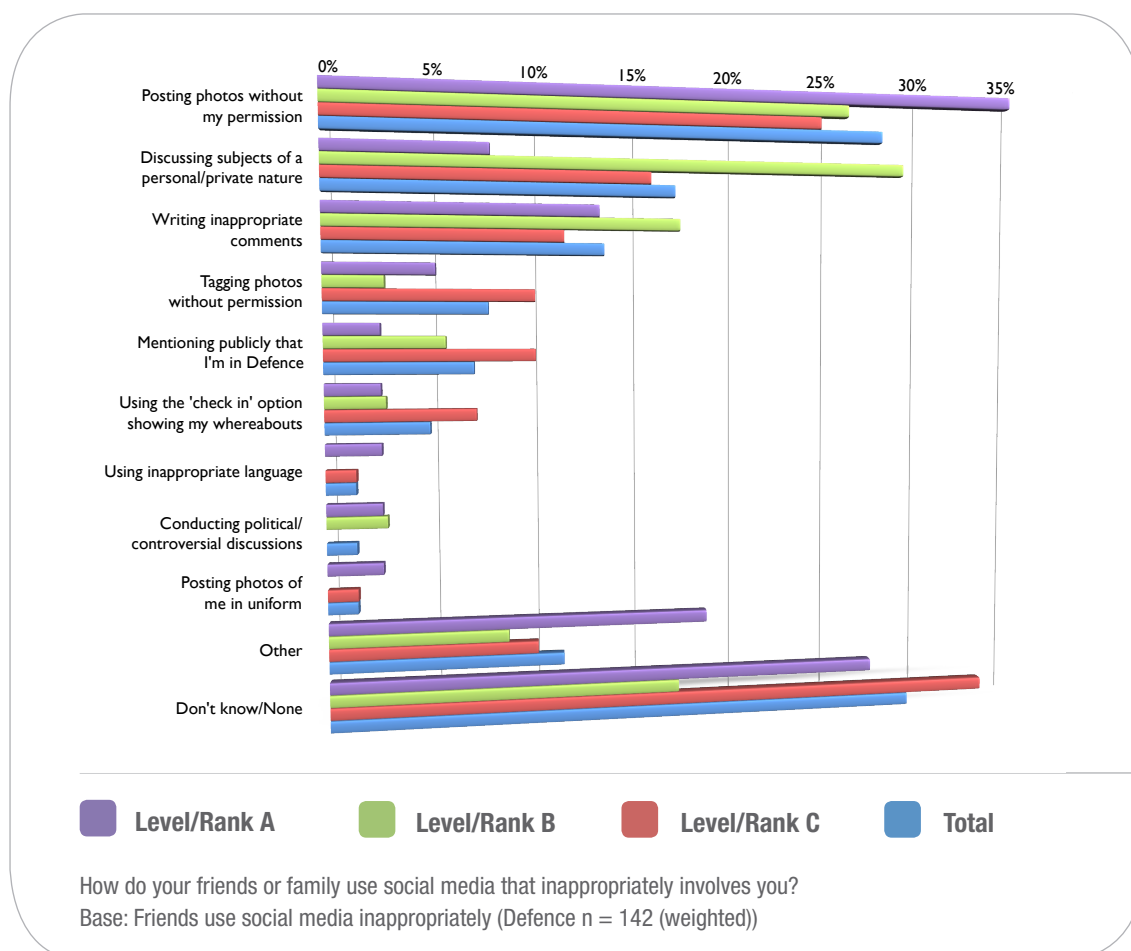
DO FRIENDS/FAMILY USE SOCIAL MEDIA THAT INAPPROPRIATELY INVOLVES YOU?



	Defence Total	A Army	A NAVY	A RAAF	A DoD	B Army	B Navy	B RAAF	B DoD	C ARMY	C NAVY	C RAAF	C DoD	Public Total	Public A	Public B	Public C	Public D
Yes	9%	11%	15%	6%	7%	13%	11%	8%	6%	9%	11%	12%	3%	11%	16%	11%	9%	11%
No	70%	67%	64%	70%	73%	64%	59%	68%	72%	72%	74%	69%	68%	68%	66%	68%	71%	67%
I don't know	21%	21%	21%	23%	20%	23%	30%	26%	22%	19%	14%	19%	28%	21%	18%	21%	20%	21%

The majority of respondents do not believe their friends or family use social media in a way that inappropriately involves them. However, just over one in five respondents (both Defence and public) are unsure either way. This increases to 28% and 30% among Level/Rank B Navy and Level/Rank C DoD respondents, respectively.

HOW DO YOUR FRIENDS/FAMILY USE SOCIAL MEDIA INAPPROPRIATELY? DEFENCE



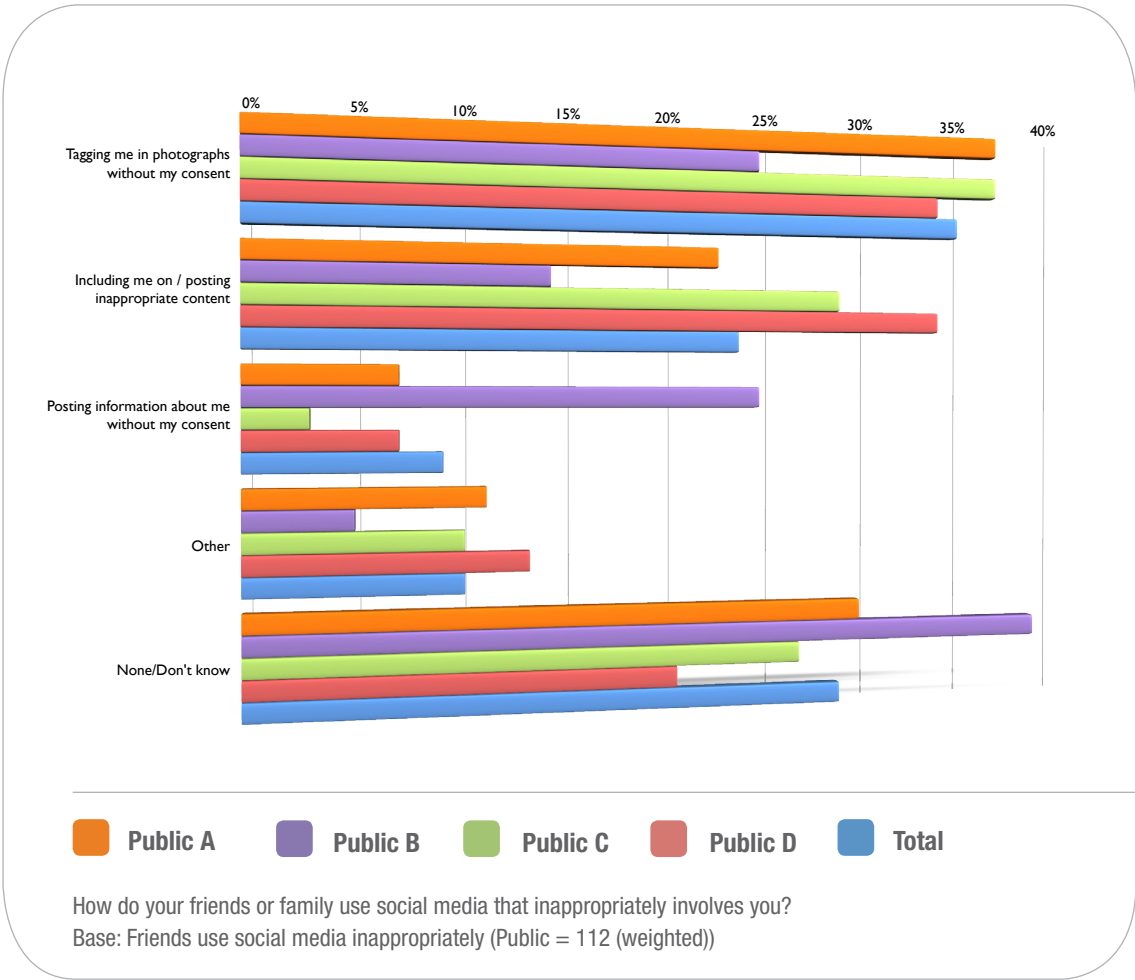
	Defence Total	Level /Rank A	Level /Rank B	Level /Rank C
Don't know/None	29%	27%	17%	33%
Other	11%	18%	9%	10%
Posting photos of me in uniform	1%	3%	0%	1%
Conducting political/ controversial discussions	1%	3%	3%	0%
Using inappropriate language	1%	3%	0%	1%
Using the 'check in' option showing my whereabouts	5%	3%	3%	7%
Mentioning publicly that I'm in Defence	7%	3%	6%	10%
Tagging photos without permission	8%	5%	3%	10%
Writing inappropriate comments	13%	13%	17%	11%
Discussing subjects of a personal/private nature	17%	8%	29%	16%
Posting photos without my permission	27%	34%	26%	24%

The biggest concern Defence employees have is that their friends/family post photos without their permission, particularly among those at Level/Rank A.

Level/Rank B employees are more concerned that their friends/family are discussing subjects of a personal nature.

Thirteen per cent of Defence personnel feel that their friends write inappropriate comments.

HOW DO YOUR FRIENDS/FAMILY USE SOCIAL MEDIA INAPPROPRIATELY? PUBLIC

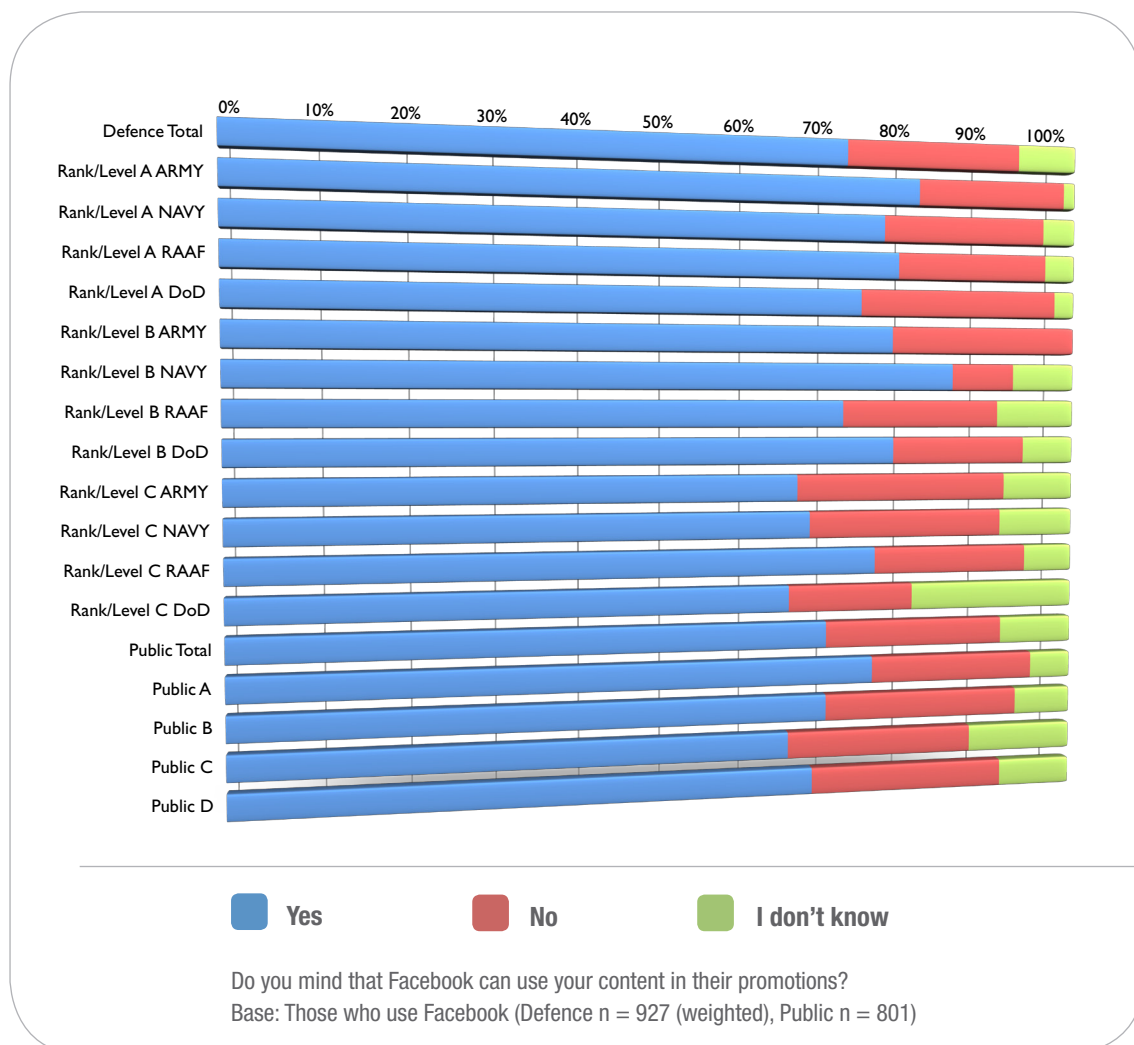


	Total	Public A	Public B	Public C	Public D
None/Don't know	28%	29%	38%	26%	20%
Other	10%	11%	5%	10%	13%
Posting information about me without my consent	9%	7%	24%	3%	7%
Including me on / posting inappropriate content	23%	22%	14%	28%	33%
Tagging me in photographs without my consent	34%	36%	24%	36%	33%

Over a third of respondents expressed concern that their friends/family were tagging them in photos without their consent.

A quarter of respondents noted that their friends/family were making inappropriate comments.

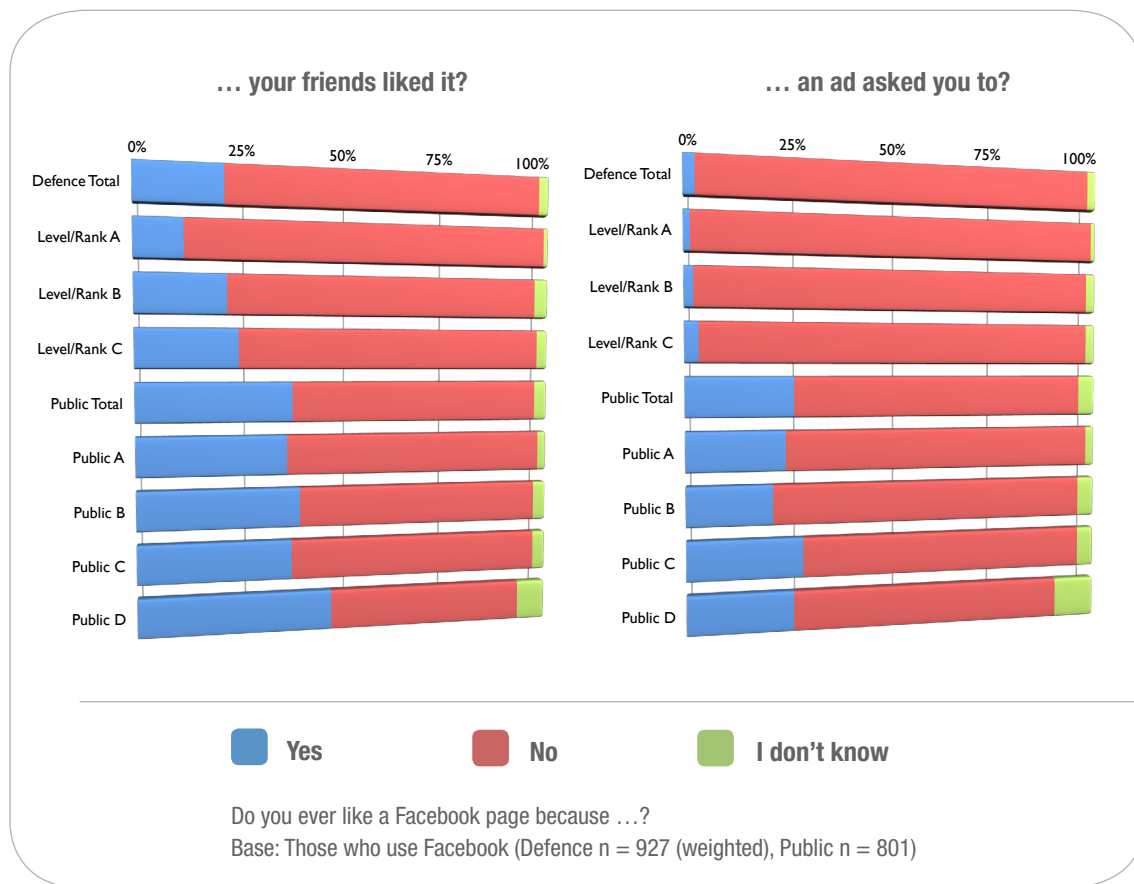
DO YOU MIND THAT FACEBOOK CAN USE YOUR CONTENT IN THEIR PROMOTIONS?



	Defence Total	A Army	A NAVY	A RAAF	A DoD	B Army	B Navy	B RAAF	B DoD	C ARMY	C NAVY	C RAAF	C DoD	Public Total	Public A	Public B	Public C	Public D
Yes	71%	80%	76%	78%	73%	77%	85%	71%	77%	66%	67%	75%	64%	69%	74%	69%	65%	68%
No	21%	18%	20%	19%	24%	23%	8%	19%	16%	26%	24%	19%	15%	22%	20%	24%	23%	24%
I don't know	7%	1%	4%	4%	2%	0%	8%	10%	6%	9%	9%	6%	20%	9%	5%	7%	13%	9%

Defence and the public are in agreement when it comes to Facebook using their content in its promotions. Around seven in 10 respondents indicate that they do not like it.

DO YOU EVER 'LIKE' A FACEBOOK PAGE BECAUSE...



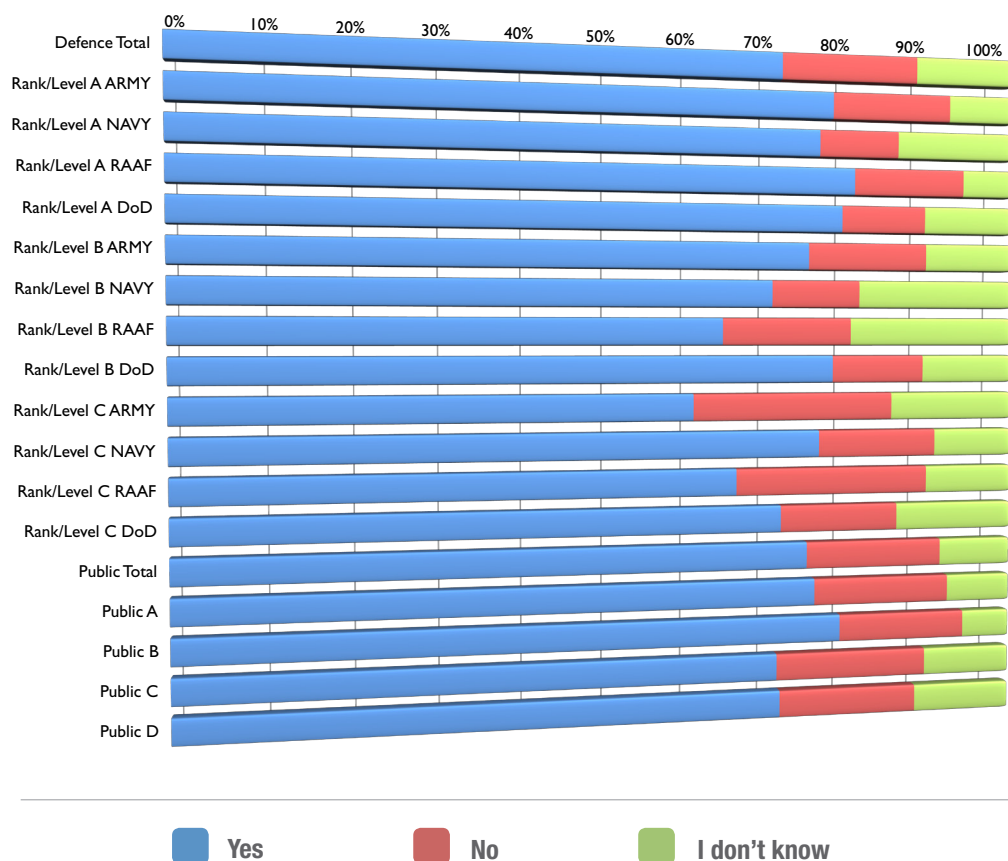
Friends liked it	Defence Total	Level/Rank A	Level/Rank B	Level/Rank C	Public Total	Public A	Public B	Public C	Public D
Yes	21%	11%	21%	24%	36%	35%	38%	36%	46%
No	77%	88%	76%	74%	60%	63%	59%	61%	48%
I don't know	2%	1%	3%	3%	3%	2%	3%	3%	7%

An ad	Defence Total	Level/Rank A	Level/Rank B	Level/Rank C	Public Total	Public A	Public B	Public C	Public D
Yes	3%	2%	2%	3%	25%	23%	20%	27%	25%
No	95%	97%	96%	94%	71%	75%	76%	69%	66%
I don't know	2%	1%	2%	2%	4%	2%	4%	4%	10%

Compared to Defence, the Australian public are significantly more likely to 'like' a Facebook page either because their friends liked it or because an advertisement asked them to. Only 3% of Defence personnel would 'like' a Facebook page if prompted to by an ad, compared to 25% of Australians.

ARE YOU CONCERNED ABOUT ...

PRIVACY SETTINGS THAT AREN'T CLEAR, SO I DON'T KNOW EXACTLY WHO CAN SEE MY POSTS AND PHOTOS?



Do the following concern you about social media usage?
Base: Total respondents (Defence n = 1574 (weighted), Public n = 1000)

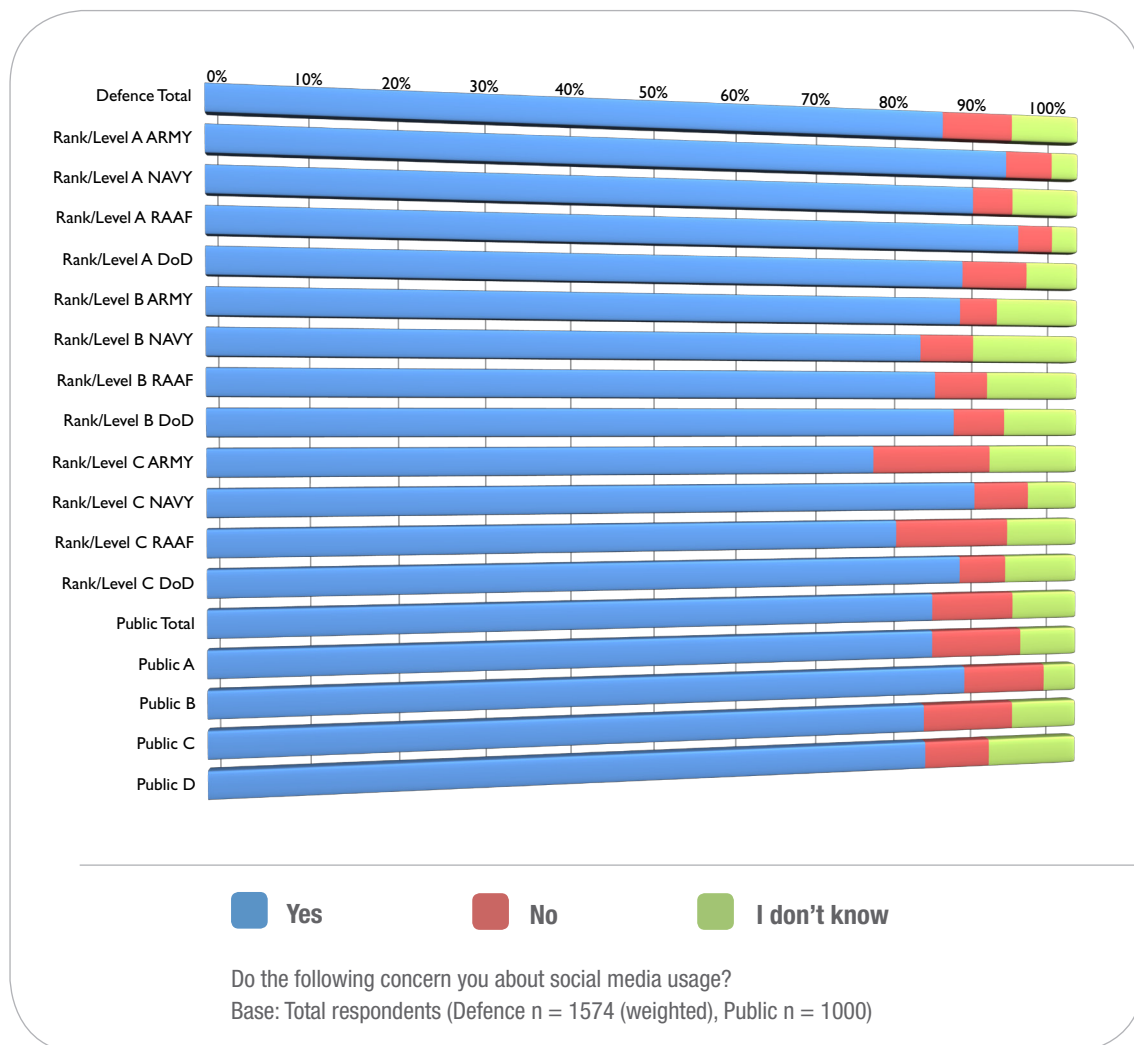
	Defence Total	A Army	A NAVY	A RAAF	A DoD	B Army	B Navy	B RAAF	B DoD	C ARMY	C NAVY	C RAAF	C DoD	Public Total	Public A	Public B	Public C	Public D
Yes	71%	77%	75%	80%	78%	74%	70%	65%	77%	60%	75%	65%	71%	74%	75%	79%	71%	70%
No	17%	15%	10%	14%	10%	15%	11%	16%	11%	25%	15%	24%	15%	17%	17%	16%	19%	17%
I don't know	12%	8%	15%	6%	11%	11%	20%	21%	11%	15%	10%	11%	15%	9%	8%	6%	11%	12%

Overall, the public are slightly more concerned than Defence employees when it comes to privacy settings in social media. However, those at Defence Level/Rank A show more concern than their Level/Rank B and C counterparts.

ARE YOU CONCERNED ABOUT ...

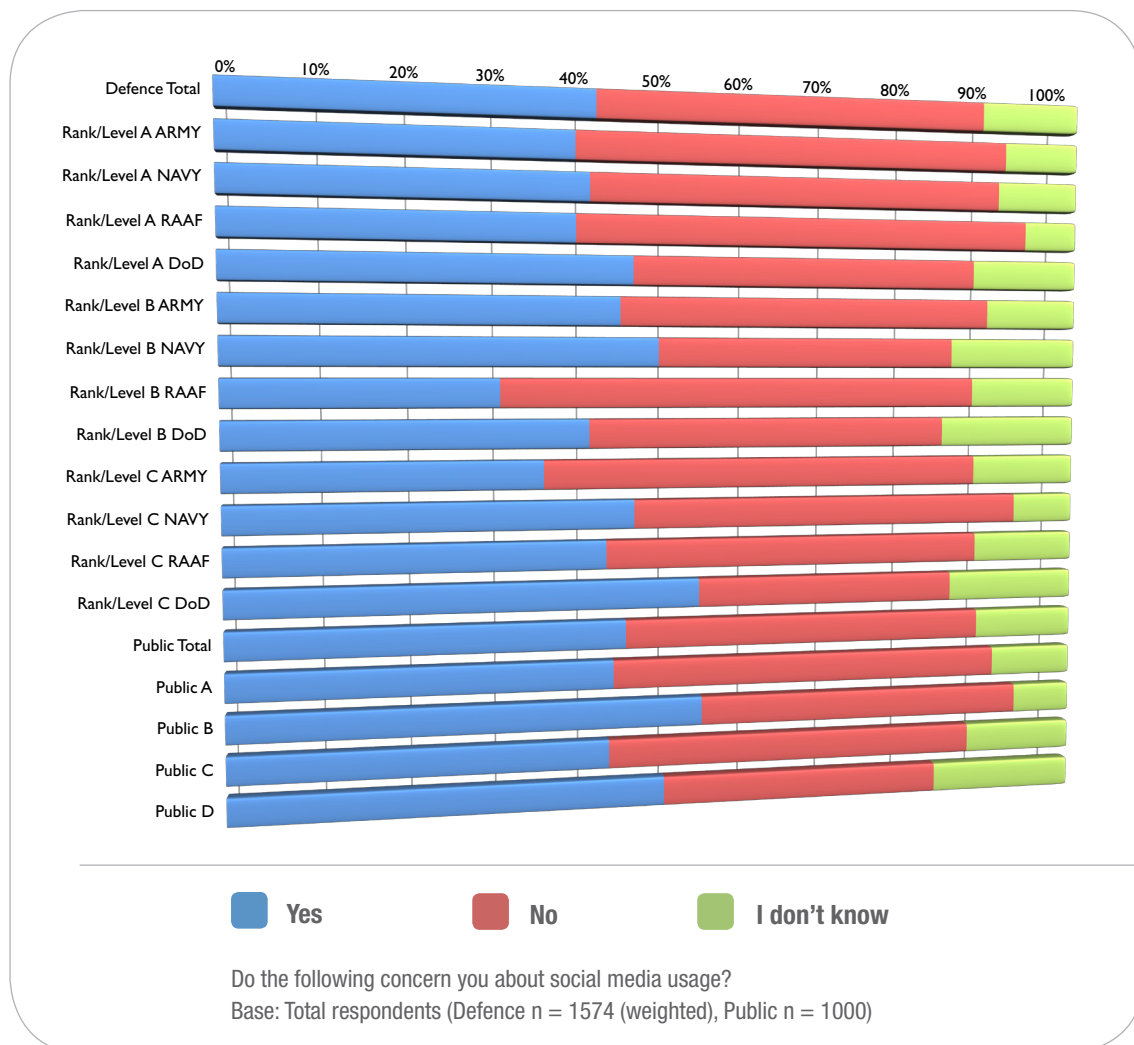
POSSIBLE SECURITY BREACHES WITH THE

SOCIAL MEDIA WEBSITES?



Worry about possible security breaches within social media is high among both the general public and Defence – more than eight out 10 respondents express their concern. This increases to over nine in 10 respondents for Level/Rank A Army and RAAF. Conversely, Army personnel at Level/Rank C show the least concern.

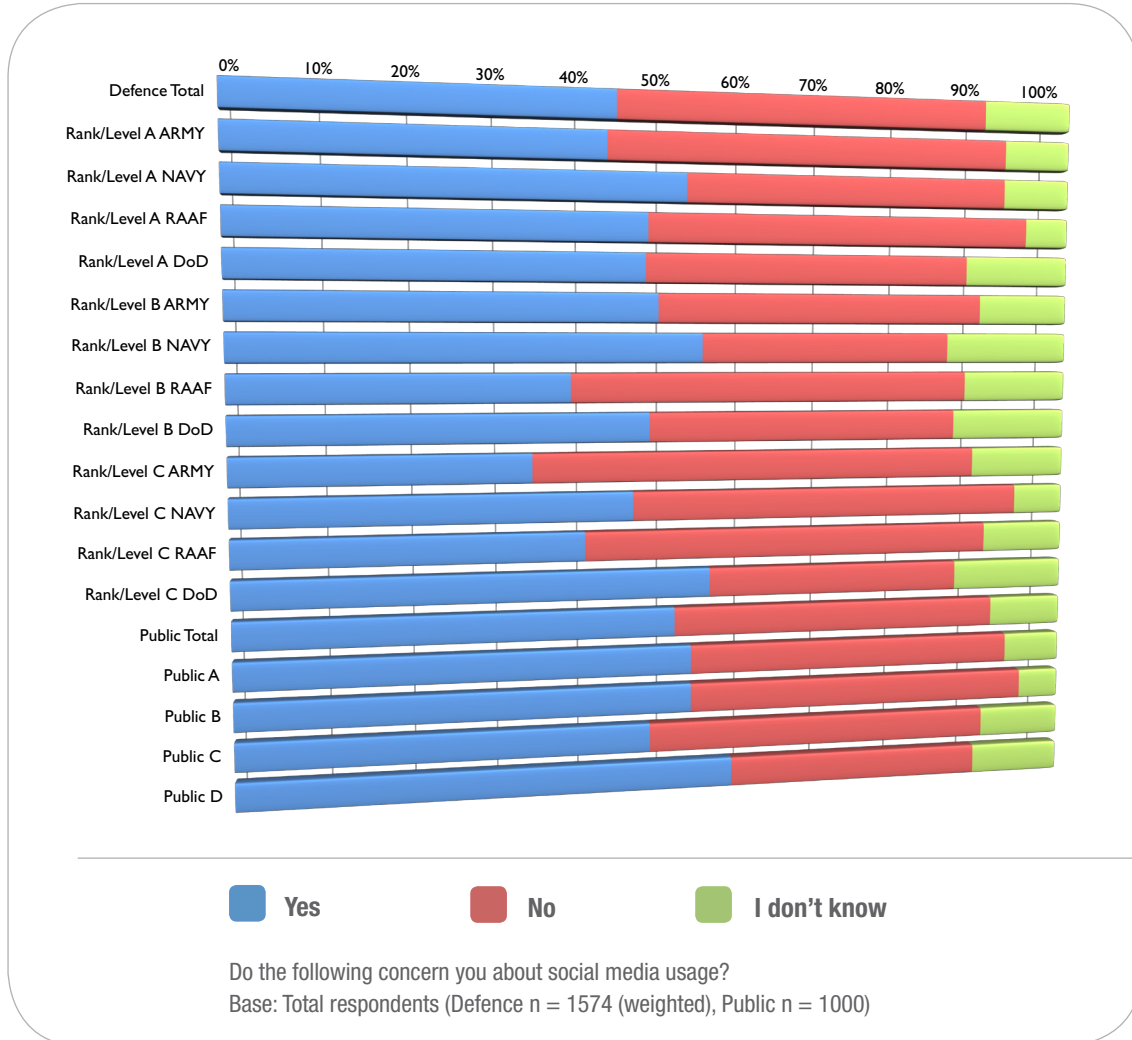
ARE YOU CONCERNED ABOUT ... CAREER IMPACT – THAT MY SUPERIORS OR COLLEAGUES CAN SEE MY POSTS OR PHOTOS AND JUDGE MY ACTIVITIES?



There is much less worry about career impacts than there is about privacy and security, and concern is slightly greater among the public than in Defence. Least concerned were those in Army Level/Rank A and C and RAAF Level/Rank B.

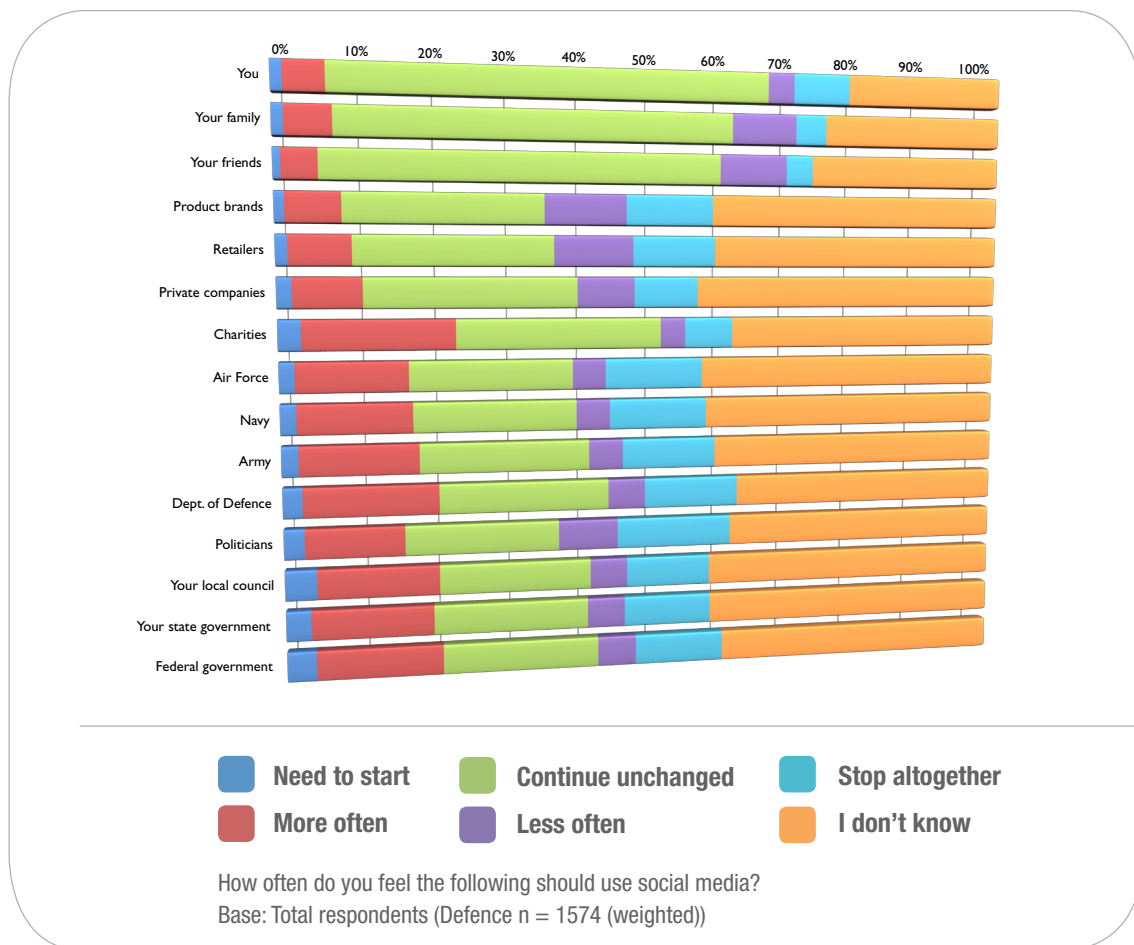
ARE YOU CONCERNED ABOUT ...

PERSONAL REPUTATION – THAT MY POSTS OR PHOTOS CAN BE JUDGED BY OTHERS?



Both Defence and public respondents show slightly more concern about their personal reputation than about career impact. Concern is greater among the general public than in Defence. A notable exception is the Army Level/Rank A group, among which the majority claim they are not concerned.

HOW OFTEN DO YOU FEEL THE FOLLOWING SHOULD USE SOCIAL MEDIA? – DEFENCE

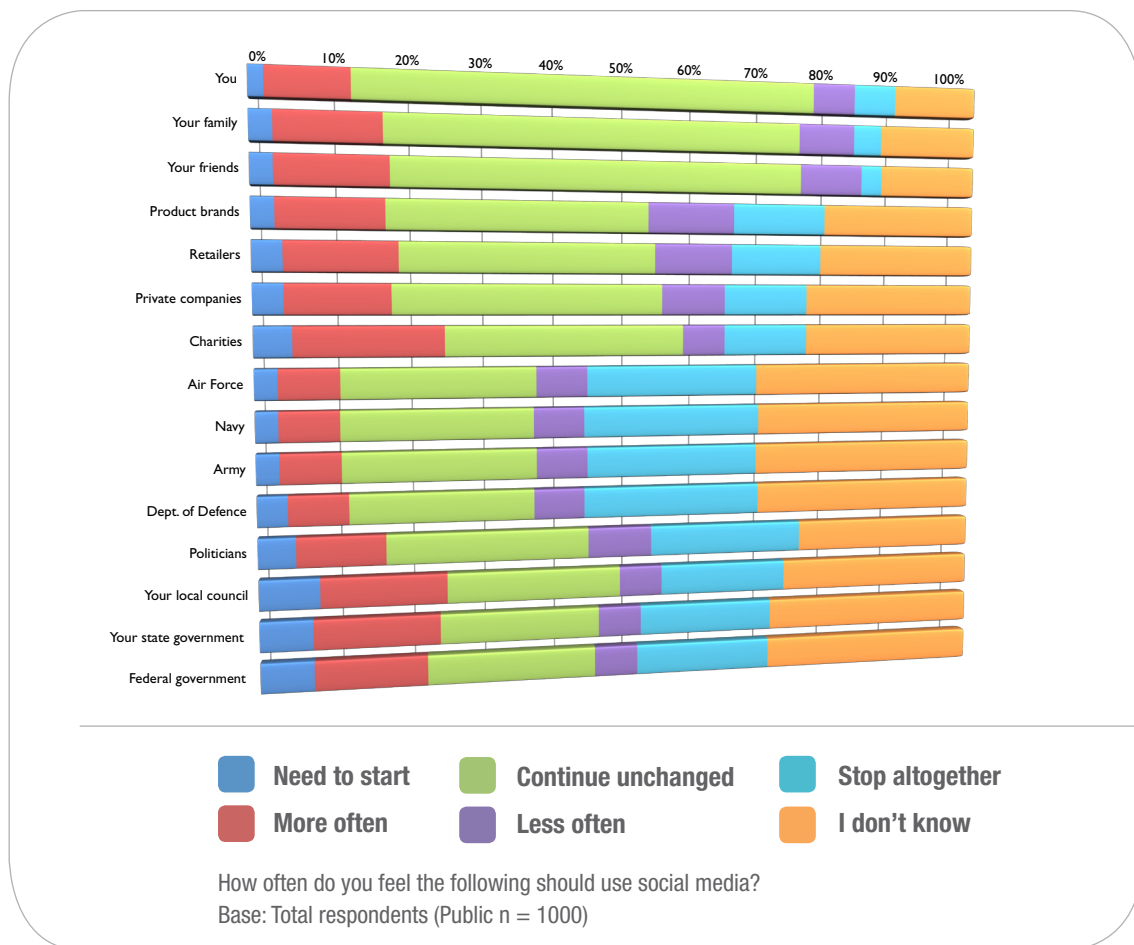


	Need to start	More often	Continue unchanged	Less often	Stop altogether	I don't know
Federal government	4%	17%	21%	5%	12%	40%
Your state government	3%	16%	21%	5%	12%	42%
Your local council	4%	16%	21%	5%	12%	42%
Politicians	3%	13%	21%	8%	16%	39%
Dept. of Defence	3%	18%	23%	5%	13%	38%
Army	2%	16%	23%	5%	13%	41%
Navy	2%	15%	22%	5%	14%	42%
Air Force	2%	15%	22%	5%	14%	43%
Charities	3%	20%	28%	3%	7%	39%
Private companies	2%	9%	29%	8%	9%	44%
Retailers	2%	8%	27%	11%	11%	41%
Product brands	1%	7%	27%	11%	12%	42%
Your friends	1%	5%	54%	9%	4%	27%
Your family	2%	6%	53%	9%	4%	25%
You	2%	5%	59%	4%	8%	22%

Most Defence employees feel that social media use by themselves, their families and their friends should continue unchanged.

Of those in the armed forces, 15–18% believe they need to use social media more often than they do now. Slightly fewer (13–14%) feel that social media use should stop altogether. Most people are undecided or feel that current usage should continue unchanged.

HOW OFTEN DO YOU FEEL THE FOLLOWING SHOULD USE SOCIAL MEDIA? – PUBLIC

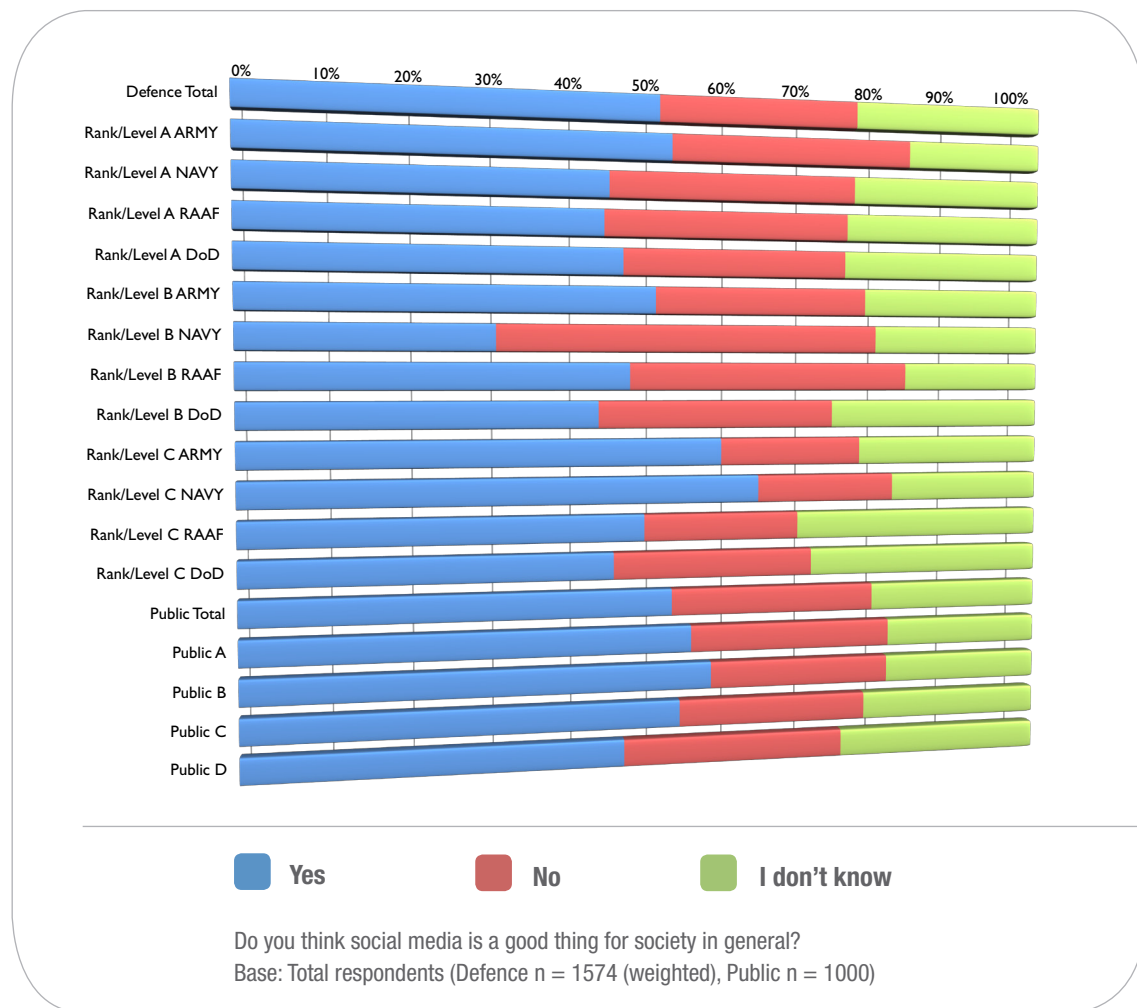


	Need to start	More often	Continue unchanged	Less often	Stop altogether	I don't know
Federal government	7%	15%	23%	6%	19%	30%
Your state government	7%	17%	22%	6%	19%	30%
Your local council	8%	17%	24%	6%	18%	28%
Politicians	5%	12%	28%	9%	22%	26%
Dept. of Defence	4%	8%	25%	7%	25%	32%
Army	3%	8%	26%	7%	24%	32%
Navy	3%	8%	26%	7%	25%	32%
Air Force	3%	8%	26%	7%	24%	32%
Charities	5%	20%	33%	6%	12%	25%
Private companies	4%	14%	37%	9%	12%	25%
Retailers	4%	15%	35%	11%	13%	23%
Product brands	3%	14%	35%	12%	13%	22%
Your friends	3%	15%	57%	9%	3%	14%
Your family	3%	14%	57%	8%	4%	14%
You	2%	11%	63%	6%	6%	12%

Around six in 10 respondents feel that their social media use, as well as that of their family and friends, should continue unchanged.

Interestingly, around a quarter of Australians believe that Defence should stop using social media altogether – a significantly higher proportion than among those employed in Defence. Fewer than one in 10 feel that Defence should increase its use of social media.

DO YOU THINK SOCIAL MEDIA IS A GOOD THING FOR SOCIETY IN GENERAL?



Around half of all respondents, both Defence and public, feel that social media is a good thing for society. Those that are most in favour of it are Defence personnel at Level/Rank C in the Army and Navy. Those most against it are Level/Rank B Navy employees, of whom fewer than one in three believe social media to be a good thing.

ANNEX 2

PUBLIC PERCEPTIONS

ANNEX 2 PUBLIC PERCEPTIONS

This review identified the current social media presences of Defence in order to understand the organisation's official penetration of social media, the coverage of unofficial pages, and the impact of unofficial pages on the brand.

The review used Alterian SM2 to analyse the period of four months between 1 March and 30 June 2011. This social media software can analyse a range of internet sites, including social networking sites such as Facebook and Twitter, news media sites and forums. While social media monitoring can be highly effective in identifying key conversations about a brand or company, it does not cover 100% of the internet and social media. In addition, limitations resulting from Facebook privacy restrictions and Twitter data purchase affect social media monitoring results. However, this type of monitoring is effective in establishing baselines and identifying trends that allow for comparisons to be drawn between datasets. Sentiment or content tone is automatically assigned by the software through keyword analysis. Keywords such as 'war' have a generally negative connotation to them (as defined by the software); however, in relation to Defence, discussion about war does not immediately signify negativity.

Although the Defence community refers to itself as 'Defence' or 'the Department of Defence', the traditional media and the general public who use social media more commonly use terms such as 'the Australian Defence Force' or 'the ADF'. For this reason, search terms such as 'ADF' and 'Australian Defence Force' were used in the monitoring, in order to gather the most appropriate public conversations.

Australian Defence Force – Public perceptions

The number of mentions in the media and the top domains data show that conversation about the ADF was driven mainly by news stories.

ADF conversation volume

Notable peaks in the data occurred on 6, 7, 11 and 12 April due to extensive media coverage of the ‘Skype incident’, which was first aired on Channel Ten news on 5 April. The incident became a major conversation driver for news.

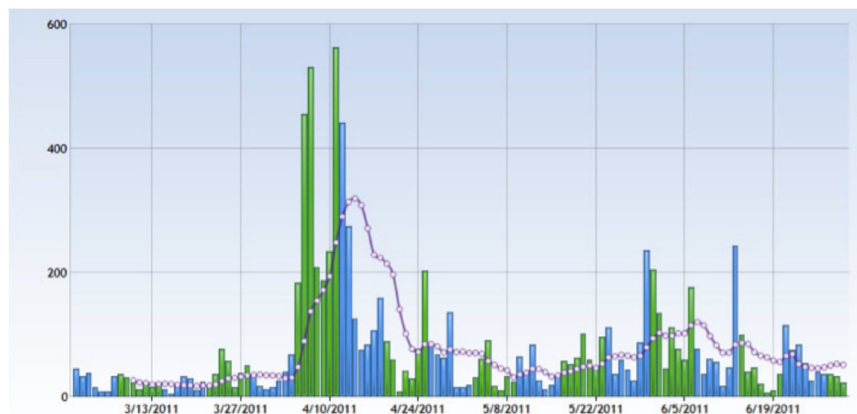


Figure A2.1: – ADF conversation volume – March to June 2011

Legend – Green and blue columns represent alternating weeks. The purple line represents a 10-day rolling average.

Social media conversation over the four-month period totalled over 9,000 mentions, with an average of 74.4 mentions per day. The highest peak of conversation occurred on 11 April 2011, when there were 562 mentions due media coverage of the Skype incident. The lowest number of mentions (4) occurred on 16 March 2011.

ADF conversation sentiment

Conversation sentiment was assigned automatically through keyword analysis. The sentiment of conversation about the ADF tended towards the negative, particularly because of recent and previous that were brought to light in the media.

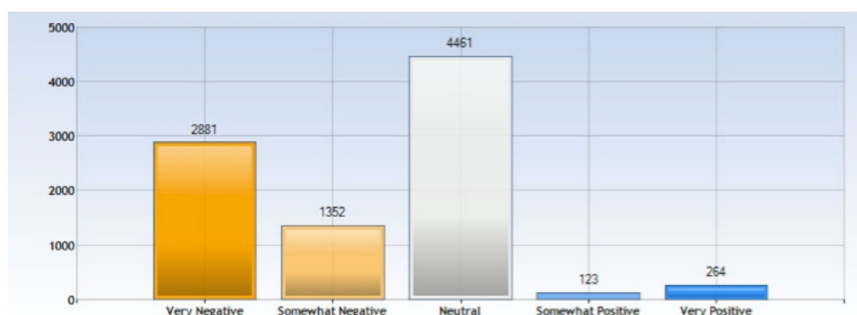


Figure A2.2: – ADF conversation sentiment – March to June 2011

Some examples of conversation are identified below.

Negative

'Weakening the ADF in the name of equality'

29 June 2011 – ABC The Drum Opinion

<http://www.abc.net.au/unleashed/2776294.html>

Weakening the ADF in the name of equality

358 Comments



So Defence Minister Stephen Smith was really serious. In recent weeks Australian Army combat units have been briefed to expect women within their ranks by next year.



This was an opinion piece published on the ABC website that criticised the ADF for letting women take positions that put them on the front line.

Females are excluded from our most violent full contact sports because we know they won't be able to survive on the footy oval or rugby pitch. In track & field, swimming and basketball, we recognise the inherent physical superiority of men over women through gender-specific categories and leagues. After all, it's not called the WNBA for nothing.

The military feminists assure us there are Australian Amazons out there just waiting for the opportunity to prove themselves in the infantry. Perhaps, but let's first test this thesis on the footy and rugby fields, where the worst thing that thrown is the occasional elbow rather than a fragmentation grenade.

The article prompted a lot of discussion: there were 358 comments on the opinion piece, some for and some against the views.

Positive / Negative

'Girls in ADFA post'

Began 24 March 2011 before the ADFA Skype incident.

<http://forums.whirlpool.net.au/archive/1665687>

[» Forums Archive](#) » [Education](#) » [Girls in ADFA](#)

Archive version | [Return to standard view](#)

User #417704 3 posts
dannfoo
Participant

Is there any girls out there in the adfa that can answer some of my questions and concerns about life in the adfa. My step daughter is going through the application process now and i would like to know what she will be in for if she is accepted

anchor: whrl.pl/RcGWRf
posted 2011-Mar-24, 2pm AEST

On 6 April, the ADFA story was brought into conversation and argued about before being closed by a moderator who asked for the Skype incident discussion to continue an already existing thread on the topic.

User #43600 23899 posts
-storm-
Moderator

This thread has now been taken over by discussion surround the recent incident at the ADFA. Please use the [existing thread](#) for same.
As such, this thread is now closed.

anchor: whrl.pl/RcH0bP
posted 2011-Apr-7, 5pm AEST

Before the Skype incident, the thread contained opinions, both positive and negative, about the treatment of females. Male and female contributors, and service members and civilians, offered opinions.

User #113483 224 posts fezel Forum Regular	I am a male, but have close friends that are either in, or have been through the ADFA. They generally seem to enjoy their experience, and I have heard that whilst it is though, and you are expected to maintain very good study habits, that it is rewarding. I have not heard of any negative experiences that are specific to girls, although I am sure that they exist similar to how they exist at university general. Good luck to her!	anchor: whrl.pl/RcGWRR posted 2011-Mar-24, 2pm AEST
User #240907 1482 posts Ned Seagoon Whirlpool Enthusiast	My niece attended the ADFA a few years ago, and ended up leaving as a broken young woman. She was physically and mentally abused, and ended up having a series of operations which took a long time and cause a lot of pain. At least the defence force picked up the tab for her medical expenses. Sorry but I cannot recommend the ADFA to any young woman.	anchor: whrl.pl/RcGWYt posted 2011-Mar-24, 2pm AEST
User #240393 338 posts isg Forum Regular	One of my close friends went to ADFA straight out of school to do an engineering degree. She's now been serving in the Navy for 6 years and has nothing but positive things to say about her time down there. If you've got a weak personality and can't accept the fact that you're in male dominated environment and might have to hear the odd snarky remark you won't survive!	anchor: whrl.pl/RcGX3r posted 2011-Mar-24, 6pm AEST

ADF share of voice – channel analysis

While it is important to note the volume of conversation about the ADF, it is also important to note the channels in which the conversation is occurring . Share of voice channel analysis assists in identifying the key channels for conversation about the ADF.

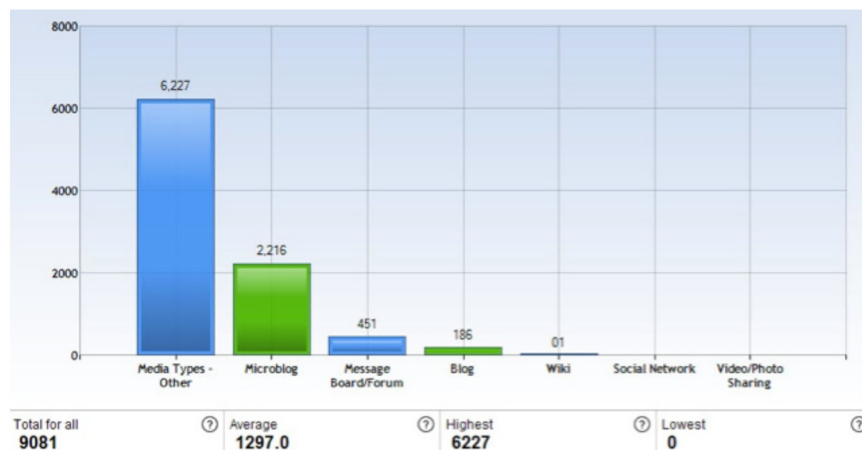


Figure A2.3: – ADF share of voice

Online media are significant contributors to the ADF conversation, mentioning the ADF 6,227 over the four month period. Four of the five top domains for ADF conversation were news sites; the other was a news site Twitter account.

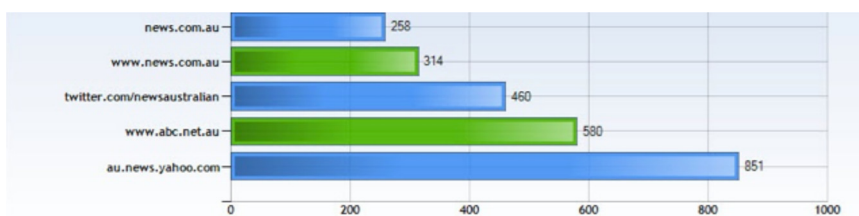


Figure A2.4: – ADF top domains for conversation

The media conversation was heavily driven by the Skype Incident and the death of servicemen overseas during the period of analysis. It is important to note that conversation on social media channels is often prompted by conversations in the traditional media.

Australian Army – Public perceptions

Australian Army mentions in the social space are significantly lower than ADF mentions as the Army is usually spoken about only when there are Army-specific issues or news reports.

Army conversation volume

Conversation volume for the Australian Army had four major peaks across the period. The peaks were due to the following events:

5 April 2011 – Sarbi the dog awarded Purple Cross

25 April 2011 – Anzac Day

4 June 2011 – Dead soldier honoured in Afghanistan

6 June 2011 – Fallen diggers arrive home

These events were discussed in the media, social networking sites and forums.

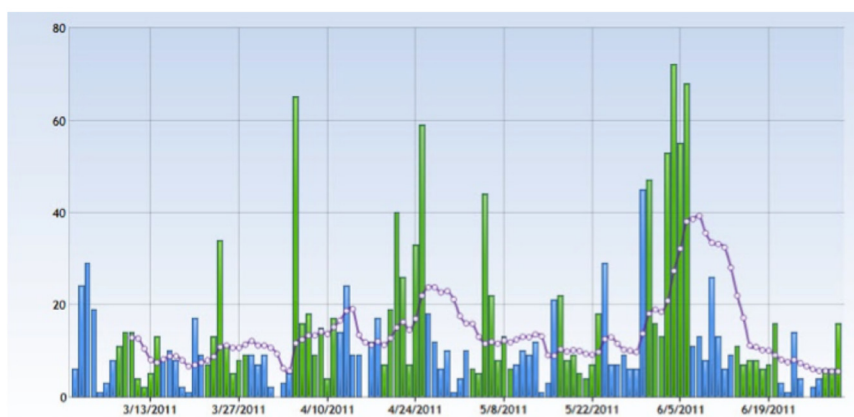


Figure A2.5: – Australian Army conversation volume – March to June 2011

Legend – Green and blue columns represent alternating weeks. The purple line represents a 10-day rolling average.

Total conversation over the period was 1,689 mentions, with an average of 13.8 mentions per day. The highest peak of conversation occurred on 4 June 2011, with 72 mentions due to the Skype incident media coverage.

Army conversation sentiment

The sentiment of conversation about the Australian Army was identified as neutral, and negative sentiment was significantly lower for the Army than for the ADF. Because conversation about the Army is driven by Army-specific events (such as the deaths and funerals of servicemen), it is important to note that no Army-specific ‘scandals’, or at least none that gained traction, appeared in the traditional media over the period.

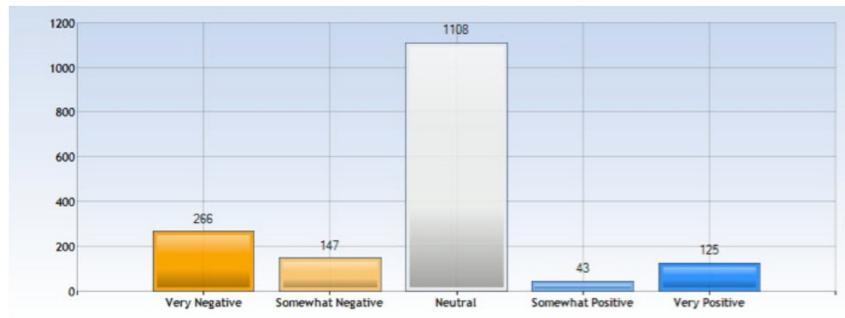


Figure A2.6: – Australian Army conversation sentiment – March to June 2011

Some examples of conversation are identified below.

Negative

Soldiers what did they die for?

31 May 2011

<http://lowyinterpreter.org/post/2011/05/31/Afghanistan-What-did-they-die-for.aspx>

This article criticises the Australian Army's continued involvement in Afghanistan. While it cannot be said to involve extreme negative sentiment, it must still be recognised as a negative opinion about the Army in the social space.

Afghanistan: What did they die for?

By Raoul Heinrichs - 31 May 2011 10:47AM

[Author profile](#)
[Previous posts](#)



It was only hours after the ramp ceremony for Australia's previous casualty in Afghanistan that the horrible news began to filter in: [another Australian soldier was dead](#), shot and killed by a rogue soldier from the Afghan National Army. This morning, a second soldier was revealed to have been killed in a helicopter crash.

Positive

Tweet by the Australian Army

1 July 2011

<http://twitter.com/#!/australianarmy/statuses/86637414403158016>

The Australian Army's contributions in the social media space were also collected by the monitoring system, so the figures for the sentiment and volume of conversation represented more than contributions by members of the general public.



It's Reserve Forces Day! Thanks to all the Reserves for your valuable contribution. If you're an Army Reservist, tell us why you joined!

1 Jul via TweetDeck ☆ Favorite ↻ Retweet ↻ Reply

Retweeted by [redacted] and 3 others



Negative

Tweet about Australian Army

30 June 2011

<http://twitter.com/#!/nattynews/statuses/86320054332964864>

Some mentions of negative sentiment should not be a major concern for the Australian Army, as members of the public merely communicate ideas or emotions that are important to them.



The Australian army fucked up my date for Friday night. I guess this is what you get when you're seeing a soldier. Mega upset :(

30 Jun via Twitter for iPhone ☆ Favorite ↻ Retweet ↩ Reply

Army share of voice – channel analysis

The share of voice channel analysis has identified where the conversation in the social space about the Australian Army was mainly occurring.

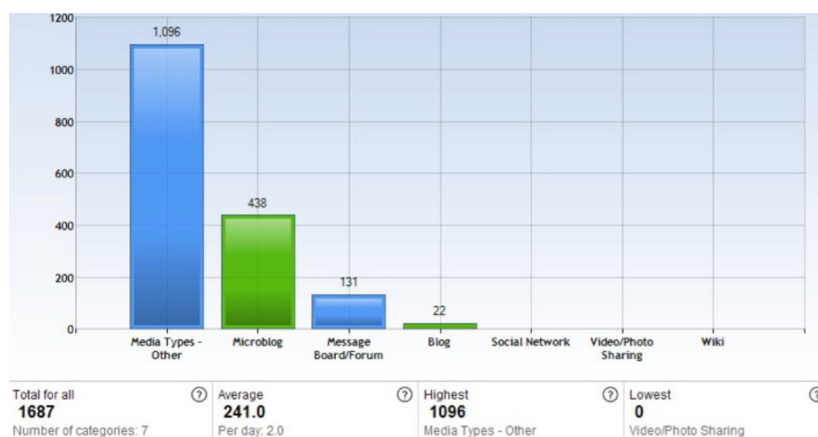


Figure A2.7: – Australian Army share of voice

The Australian Army conversation was shaped mainly by online news media, which made 1,096 mentions over the four-month period. Four of the top domains for the conversations were news sites. The remaining domain, the Australian Army Twitter account, produced 124 of the 438 microblog results for conversation. Most of the microblog conversation can be attributed to the Australian Army Twitter account in some way, as its tweets were retweeted by other Twitter users.

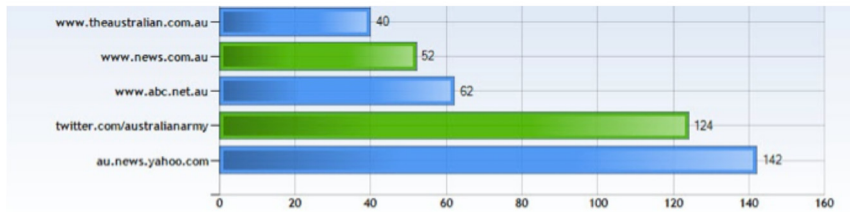


Figure A2.8: – Australian Army top domains for conversation

Royal Australian Navy – Public perceptions

As for to the Australian Army, mentions of the Royal Australian Navy in the social space are significantly fewer than mentions of the ADF. Discussion was primarily prompted by Navy-specific issues or news reports, very few which occurred or gained much traction in the March to June 2011 period.

Navy conversation volume

Conversation volume for the Royal Australian Navy had three major peaks across the period. The peaks were due to the following events:

14 April 2011 – Australian Navy rescues hostage from pirates / US sub visits Brisbane

25 April 2011 – Anzac Day

5 May 2011 – WWI digger dies

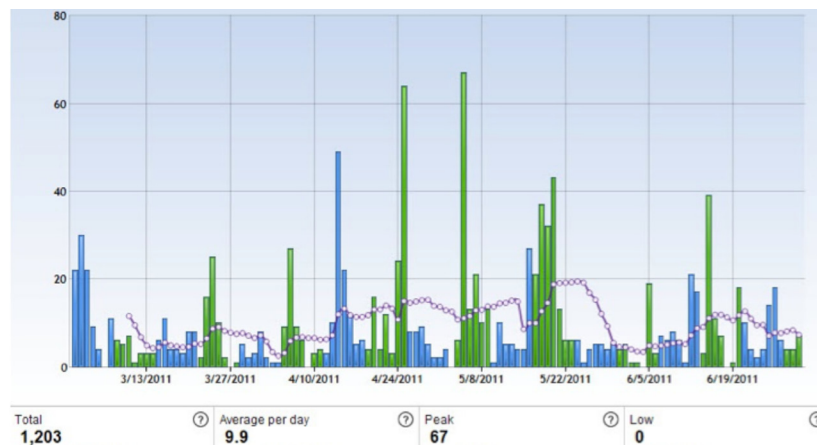


Figure A2.9: – Royal Australian Navy conversation volume – March to June 2011

Legend – Green and blue columns represent alternating weeks. The purple line represents a 10-day rolling average.

Conversation over the period total over 1,203 mentions, with an average of 9.9 mentions per day. The highest peak of conversation occurred on 5 May 2011, with 67 mentions due to the death of a 110-year-old World War I Navy veteran.

Navy conversation tone

The tone of conversation about the Royal Australian Navy was mainly neutral. As with the case of the Australian Army, the negative sentiment was significantly lower in comparison to overall ADF results. Conversation was driven by events, and the lack of Navy-specific ‘scandals’ was a contributing factor to the low volume of conversation and low volume of negative sentiment.

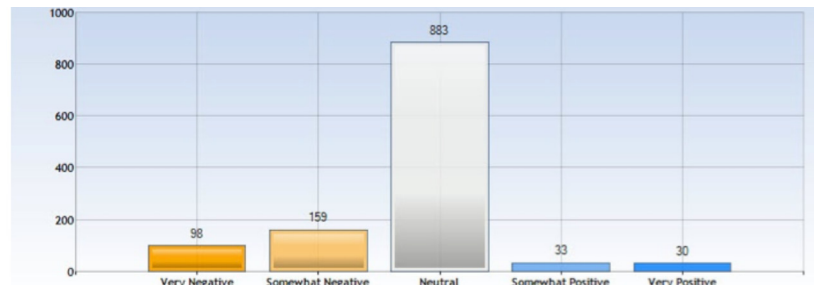


Figure A2.10: – Royal Australian Navy conversation sentiment – March to June 2011

Some examples of conversation are identified below.

Negative

*Tweet at the Royal Australian Navy and Australian Army
7 April 2011*

<http://twitter.com/#!/melwuv/statuses/55975108531077120>

This tweet was from a member of the general public, in relation to the Skype incident. The tweet was about the Services taking responsibility for the actions of the cadets.



Negative

*The Royal Australian Navy should urgently return to Thursday Island off Cape York,
Warren Entsch says*

27 June 2011

<http://www.theaustralian.com.au/national-affairs/defence/navy-thursday-island/story-e6frg8yo-1226082641300>

The news article discusses the need for Thursday Island to be protected by the Royal Australian Navy, as it left a gap in the defence of the country. This article criticises the withdrawal by the Navy in 2010.

The Royal Australian Navy should urgently return to Thursday Island off Cape York, Warren Entsch says

Mark Dodd | The Australian | June 27, 2011 10:45AM

Share

Recommend

Send

20 people recommend this. Be the first of your friends.

5 retweet

Share

THE Royal Australian Navy should urgently re-establish a naval presence on Thursday Island off Cape York or risk a major border security breach across the Torres Strait, a senior federal opposition MP has warned.

Positive

Navy culture very good, says chief

29 April 2011

<http://www.theage.com.au/national/navy-culture-very-good-says-chief-20110428-1dyw4.html>

Rear Admiral Steve Gilmore defended the Navy culture in an article, in response to comments from the general public regarding the Skype incident and the HMAS *success* report.

Navy culture very good, says chief

Dan Oakes Aqaba
April 29, 2011

The commander of the Royal Australian Navy's fleet has made an impassioned defence of navy culture as a number of inquiries begin into the treatment of women in the Defence Force.

Navy share of voice – channel analysis

Share of voice channel analysis of identified where the Royal Australian Navy conversation in the social space was occurring.

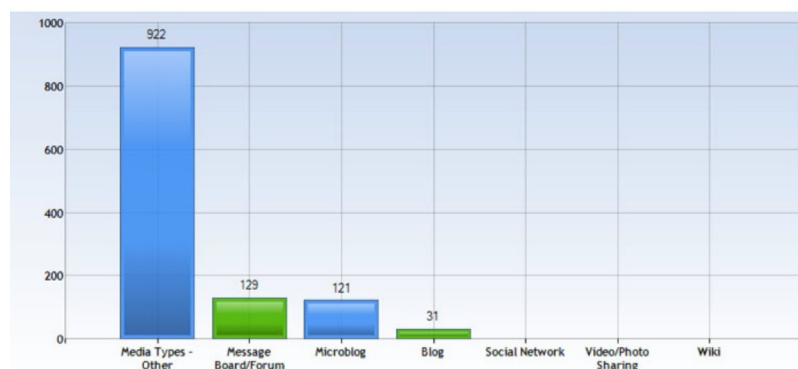


Figure A2.11: – Royal Australian Navy share of voice

Media was the main channel for conversation about the Navy, with 1,203 mentions over the four month period. Four of the top five domains for the conversation were online news sites. The fifth was the 'Defence Talk' forum, in which there were a range of military discussions in the 'Royal Australian Navy Discussions and Updates' category.

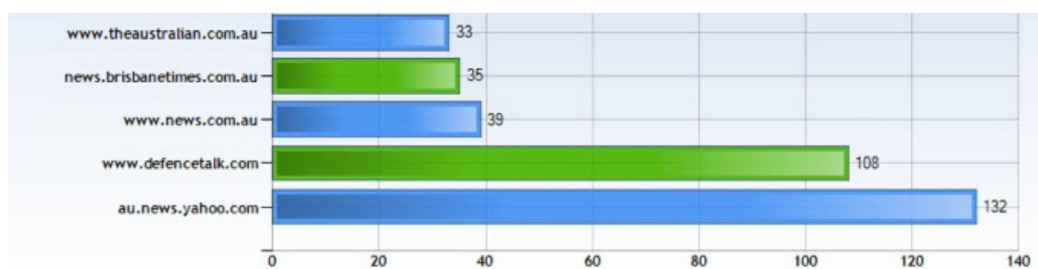


Figure A2.12: – Royal Australian Navy top domains for conversation

Royal Australian Air Force – Public perceptions

RAAF conversation mentions were significantly lower in volume than those for the ADF. Discussion was primarily prompted by Air Force-specific issues or news reports. In the Skype incident, the female at the centre of the incident was identified as an RAAF cadet. It is for this reason that the RAAF conversation was notably higher than that for the Army or Navy.

RAAF conversation volume

RAAF conversation had three major peaks across the period. The peaks were due to the following events:

30 March 2011 – RAAF marks 90 years of flying

24 April 2011 – Pre Anzac Day news material

18 May 2011 – RAAF Roulette plane crash at East Sale base Victoria

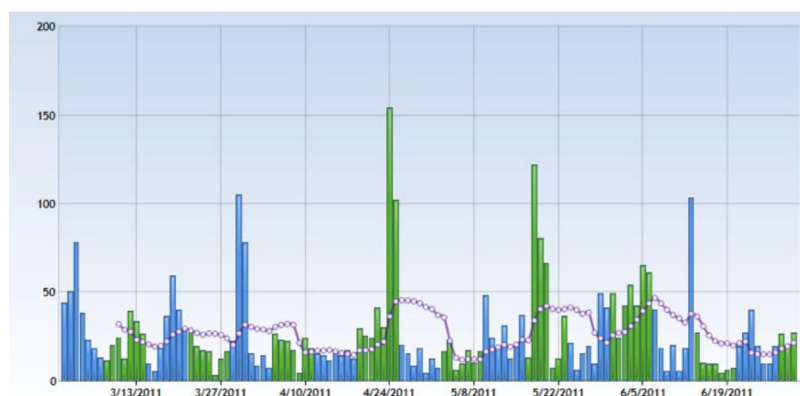


Figure A2.13: – Royal Australian Navy conversation volume – March to June 2011

Legend – Green and blue columns represent alternating weeks. The purple line represents a 10-day rolling average.

Total conversation over the period of four months gathered by the system was 3,322 mentions, with an average of 27.2 mentions per day. The highest peak of conversation occurred on 24 April 2011, with 154 mentions (the day before Anzac Day). The lowest number of mentions (4) occurred on 16 March 2011.

RAAF conversation sentiment

RAAF conversation sentiment was primarily neutral. Similar to the Army and Navy results, negative sentiment for RAAF was significantly lower than for the ADF. Conversation was driven by events, and the RAAF connection in the Skype incident raised the number of mentions.

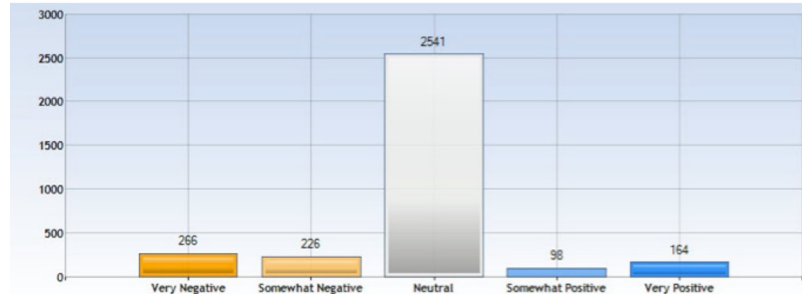


Figure A2.14: – Royal Australian Air Force conversation sentiment – March to June 2011

Some examples of conversation are identified below.

Negative

Fuel failure led to crash at RAAF East Sale

6 June 2011

<http://news.smh.com.au/breaking-news-national/faulty-fuel-system-behind-raaf-crash-20110606-1fo98.html>

The article was identified as having negative sentiment due to the words ‘crash’ and ‘injuries’.

Faulty fuel system behind RAAF crash

June 6, 2011

AAP

A faulty fuel system caused a Royal Australian Air Force plane to crash at a Victorian military base last month.

Positive

Tweet at the RAAF's twitter account

5 May 2011

<http://twitter.com/#!/twileague/statuses/65990796217827329>

This tweet was identified as having positive sentiment due to the word ‘proud’.



RAAF share of voice – channel analysis

Share of voice channel analysis identified where the RAAF conversation in the social space was occurring.

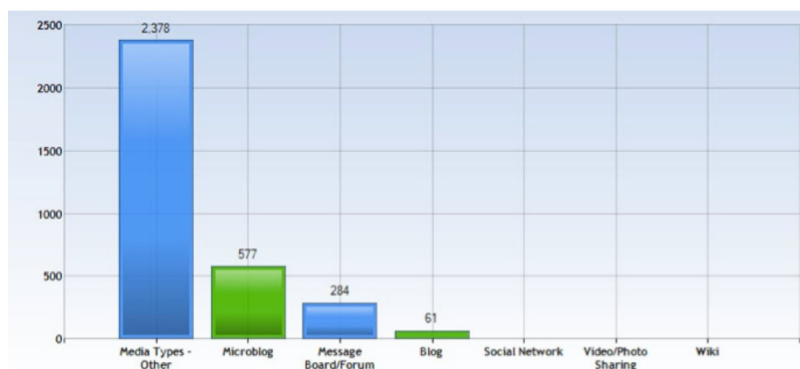


Figure A2.15: – Royal Australian Air Force share of voice

Media was the main channel for conversation about the Navy, with 2,378 mentions over the four month period. Four of the top five domains for the conversation were online news sites; the other was *Australian Aviation* magazine.

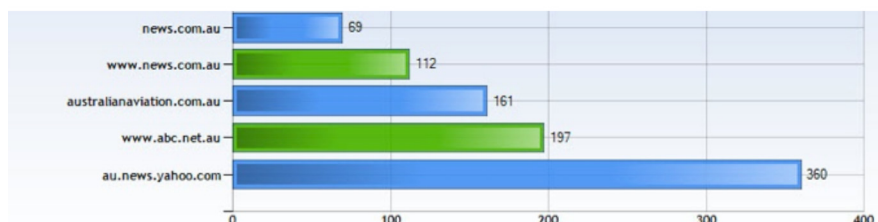


Figure A2.16: – Royal Australian Air Force top domains for conversation

News - The conversation catalyst

The social media monitoring data in this review demonstrated that the conversation about Defence during the four month reviewed was primarily driven by the traditional media and online news. Four of the five top domains for the conversation were online news sites, which contributed an overwhelming amount of conversation compared to other channels, such as microblogs or forums. The discussions in forums and microblogs and Twitter retweets about Defence were driven by reports in the media.

Sentiment - Defence contributes positively

When Defence self-promotes in the social media space, and those mentions are assigned positive sentiment by the monitoring software. Most mentions for the Australian Army in microblogs were tweets by the official Australian Army Twitter account, or retweets of that material by other users. It is important to discount the contribution by the brand itself when discussing levels of positive sentiment.

Conversation - not all about Skype

Positive conversation about Defence generally concerned events such as Anzac Day or medal awarding ceremonies. The review of public conversation indicated that conversation about all three Services was more widespread just before and on Anzac Day.

ANNEX 3: OFFICIAL AND UNOFFICIAL SOCIAL MEDIA CHANNELS

The audit covered the ADF's presences on Facebook (pages and groups), Twitter, Flickr and YouTube.

Most of the audit of social media channels was conducted on 20, 21 and 22 July 2011. This section examines the social media accounts for the ADF, the RAN, the Australian Army and the RAAF. The list is not exhaustive, but provides a sample of the official and unofficial social media presences of the ADF and the Services.

Facebook (pages)

It is unclear whether an official Facebook page exists for the ADF, as there is no link on the official website and no pages found in a Facebook search identify themselves as official. A number of unofficial ADF pages appear in the Facebook search results.



Facebook (groups)

There are a number of unofficial Facebook groups with varying levels of Facebook security. Some are the older style that resembles pages and are soon to be archived.

The screenshot shows the Facebook interface with a search bar at the top containing the text 'australian defence force'. On the left sidebar, the 'Groups' tab is selected. The main content area displays a list of search results for Facebook groups. Each result includes a profile picture, the group name, its category (e.g., 'Organizations', 'Just for Fun', 'Common Interest', 'Student Groups'), the number of members, and a button to join or request to join.

Group Name	Category	Members	Action
Australian defence force		9 members	Request to Join
Australian Defence Force Cadets	Organizations	2 members	Request to Join
Australian Defence Force Watch		2 members	Request to Join
Australian Defence Force Snipers	Organizations	57 members	Join Group
Australian Defence Force Fans!!!	Just for Fun	156 members	Join Group
Australian Defence Force Cadets	Organizations	240 members	Join Group
Australian Defence Force _ FTW!	Just for Fun	56 members	Join Group
Australian Arrogance Defence Force		20 members	Request to Join
Australian Duck Defence Force		8 members	Request to Join
Australian Defence Force Cadets (ADFC)		127 members	Request to Join
Australian Defence Force Army Wives	Common Interest	786 members	Join Group
help the Australian Defence Force	Organizations	9 members	Join Group
[ADF] Australian Defence Force Clan	Internet & Technology	8 members	Join Group
Future Australian Defence Force recruits	Student Groups	70 members	Join Group

Twitter

**@AusDefenceForce -
(AusDefenceForce)**

2,135 followers
39 following
416 tweets

[http://twitter.com/#!/
ausdefenceforce](http://twitter.com/#!/ausdefenceforce)



Features:

- Official account for ADF.
- Last tweet 21 April 2011.
- Uses #ADF hashtag in most tweets for promotion.
- Does not appear to be responding to or interacting much with other Twitter users.
- Using bit.ly links to track click-throughs.

Twitter

**@DefenceJobsAus
(DefenceJobs)**

91 followers
0 following
Locked account

[http://twitter.com/#!/
defencejobsaus](http://twitter.com/#!/defencejobsaus)



Screenshot, 22 July 2011

Features:

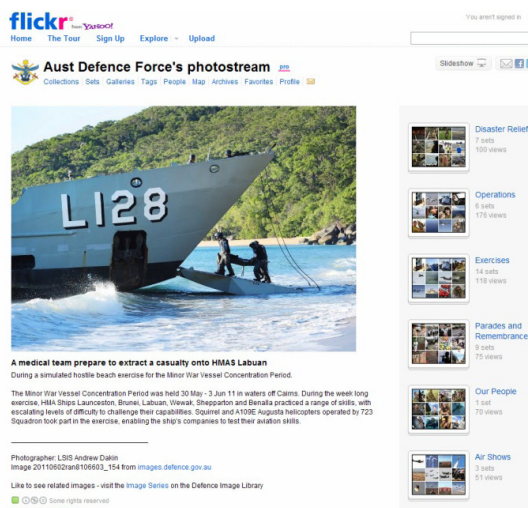
- Locked account, meaning that Twitter users have to send a request to follow and be approved by the @DefenceJobsAus administrator.
- Because the account is locked, its purpose is not clear.
- This is a closed trial from around 12 months ago.

Flickr

Aust Defence Force

Joined July 2010
1,011 items on Flickr

www.flickr.com/photos/Aus_Defence_Force



Screenshot, 22 July 2011

Features:

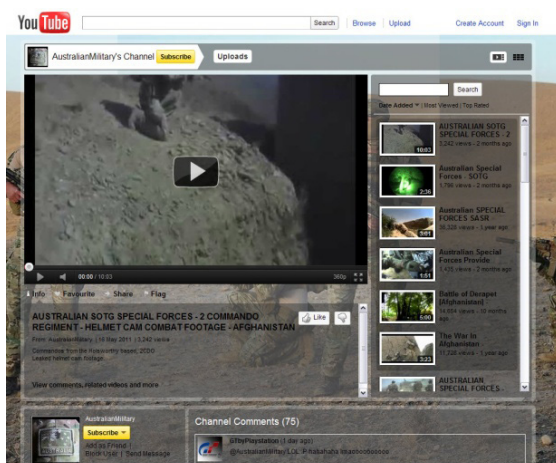
- Official Flickr presence of the ADF.
- Examples of photo content
 - disaster relief
 - exercises
 - operations
 - education and training.
- High-quality images, which contributes to the professionalism and reputation of the account.
- Appropriate stories or comments with photos help the viewer to understand the story.
- 'Our People' section shows images of service members, their rank, last name, location of work and what they do – potentially providing a little too much information.

YouTube

AustralianMilitary

Channel views – 7,265
Total upload views –
145,387
Subscribers – 332

www.youtube.com/user/AustralianMilitary



Screenshot, 22 July 2011

Features:

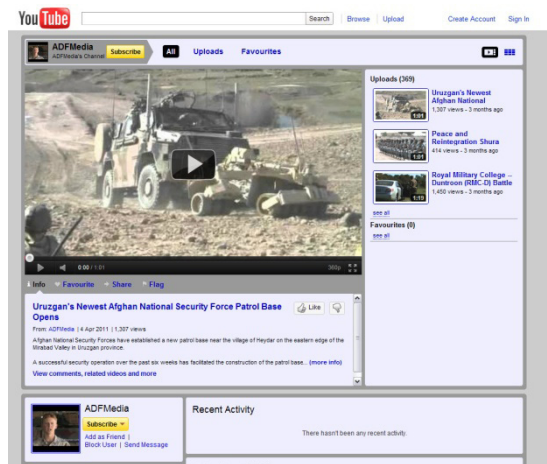
- Unofficial account.
- Unclear who runs the channel
- Not monitored – inappropriate and hateful language is used in channel comments by other users.
- Examples of video content
 - 'leaked' helmet camera footage in Afghanistan
 - Battle of Derapet (Afghanistan)
 - Australian Special Forces SASR
 - AC/DC band (live, Sydney)
 - Operation Zamarai Lor – Australia.

YouTube

ADF Media

Channel views – 79,034
Total upload views – 145,387
Subscribers – 1,414

[www.youtube.com/
user/ADFmedia](http://www.youtube.com/user/ADFmedia)



Screenshot, 22 July 2011

Features:

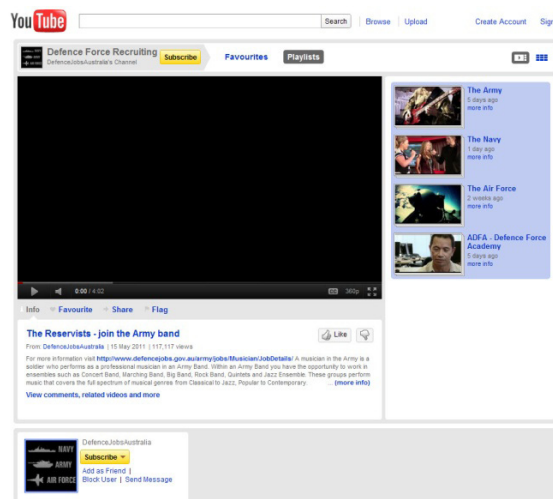
- Official account.
- Examples of video content
 - Exercise Shaggy Ridge
 - Royal Military College – Duntroon
 - Operation Pacific Assist Okinawa.
- Comments disabled for videos.
- Detailed description for each video.

YouTube

Defence Force Recruiting

Channel views – 44,288
Total upload views – 602,477
Subscribers – 605

[www.youtube.com/user/
Defencejobsaustralia](http://www.youtube.com/user/Defencejobsaustralia)



Features:

- Official channel.
- Posted videos of different types of jobs in Defence and recruitment events.
- Comments enabled on videos
 - most do not have any comments
 - those that do include arguments about joining Defence or positive comments from people waiting to join.
- Needs monitoring.

2.3.2 Royal Australian Navy

The audit for the RAN covered its presences in Facebook (pages and groups), Twitter and YouTube.

Facebook (pages)

Royal Australian
Navy

9,023 likes

[www.facebook.com/
RoyalAustralianNavy](http://www.facebook.com/RoyalAustralianNavy)



Screenshot, 20 July 2011

Features:

- Created new page in February 2011; did not start posting until 7 July 2011.
- Old page facebook.com/AustralianNavy.
- Facebook moved likes from old page to new page.
- Made new page to include 'royal' in the URL.



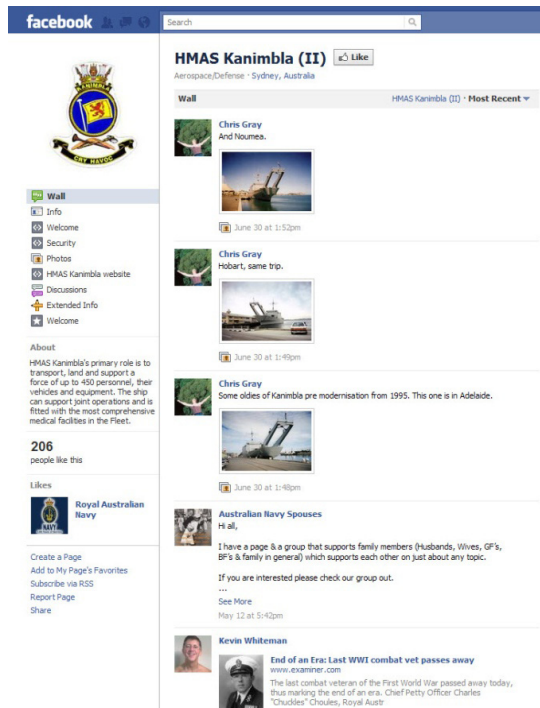
- Posting images, content from Navy website and YouTube videos.
- Responding to questions.
- Nice feel overall.
- Doing a good job.
- Need to improve the technical implementation of custom content pages.
- Staying safe online page.

Facebook (pages)

HMAS Kanimbla (II)

206 likes

www.facebook.com/HMASKanimblall



Screenshot, 22 July 2011

Features:

- HMAS Kanimbla's official fan page.
- Two Welcome pages – one says 'Access denied' when clicked.
- Security page contains broken links and the PDF download does not seem to work properly.
- Only four photos on the page (submitted by public).
- HMAS Kanimbla web page contains a link to the page.
- 'Extended info' page is blank.

HMAS Melbourne (III)

541 likes

www.facebook.com/HMASMelbournelll



Screenshot, 22 July 2011

Features:

- HMAS Melbourne's official fan page.
- Last updated March 2011.
- Includes a guide to posting.
- Security page contains broken links and the PDF download does not seem to work properly.
- Only four photos on the page (submitted by public).
- Video interviews uploaded.
- HMAS Melbourne web page contains a link to the page.
- Posting links to navy.gov.au.
- Posting photos.
- Outdated reference to 'become a fan'.

Become a fan to connect with HMAS Melbourne ship's company, family and friends.

Facebook (pages)

HMAS Tobruk (II)

230 likes

<http://www.facebook.com/HMASTobrukII>



Screenshot, 22 July 2011

Features:

- Official page.
- Welcome landing page.
- Security page contains broken links and the PDF download does not seem to work properly.
- Limited photo content.

Royal Australian Navy History

606 likes

www.facebook.com/RANHistory



Screenshot, 22 July 2011

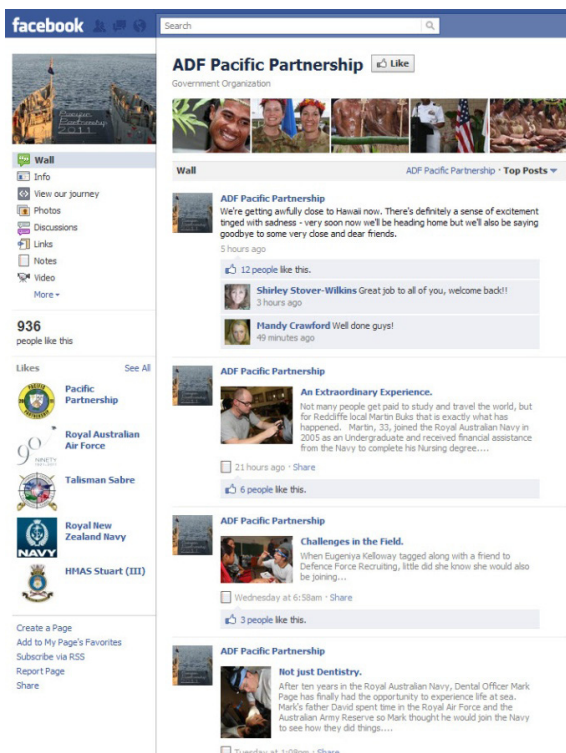
Features:

- Official page.
- Public posting photos on the page.
- Includes a guide to posting.
- Updating is inconsistent and sporadic.

ADF Pacific Partnership

936 likes

www.facebook.com/ADFPacificPartnership



Screenshot, 22 July 2011

Features:

- Official page.
- Includes a guide to posting.
- Interactive map of journey – low quality.
- Text-based Welcome page
- Photos of journey and videos posted.
- Regular updating with posts or notes.
- Stay-safe online PDF download.

HMAS Stuart (III)

163 likes

www.facebook.com/HMAStuartIII

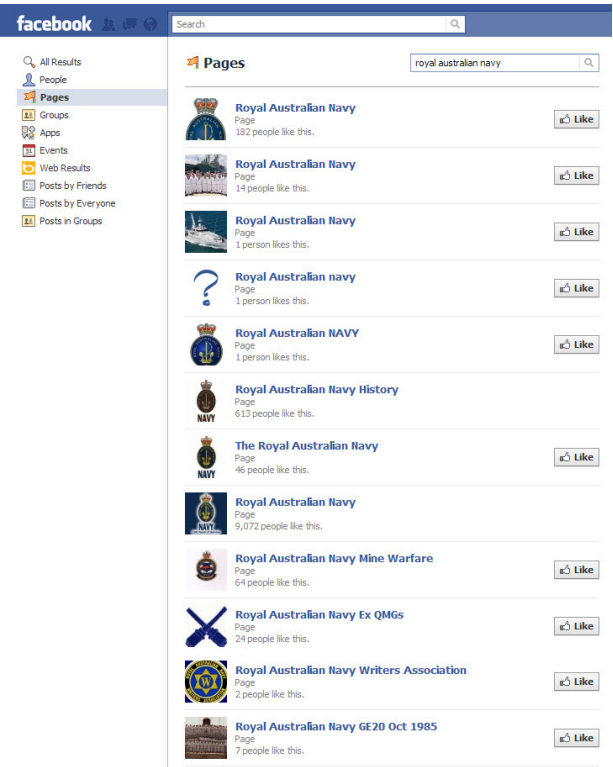


Screenshot, 22 July 2011

Features:

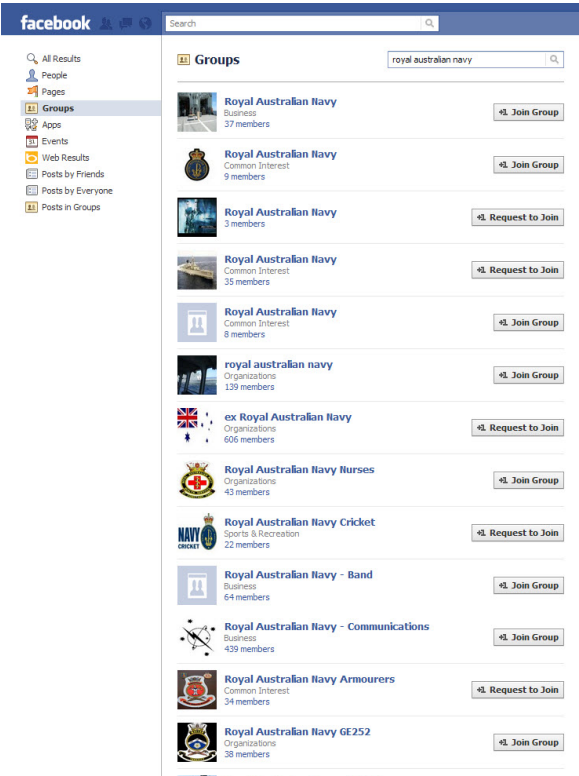
- Official page.
- Outdated reference to 'Become a fan'.
- Includes guidelines for posting.
- Security page contains broken links and the PDF download does not seem to work properly.
- Limited photo content.
- HMAS Stuart web page contains a link to the page.
- Last updated 25 April 2011.

A number of unofficial RAN pages appear in the Facebook search results alongside official pages. Some of the pages reference the RAN in inappropriate ways. The following image is a sample of the Facebook search results.



Facebook (groups)

There are a number of unofficial Facebook groups with varying levels of Facebook security. Some of the groups are the older style, which resembles pages, and are soon to be archived by Facebook.



Twitter

@Australian_Navy
(Navy Webmaster)

1,836 followers
15 following
1,372 tweets

twitter.com/#!/australian_
navy

Navy Webmaster
@Australian_Navy Australia
Official Royal Australian Navy Twitter sharing information about the Royal Australian Navy around the world.
<http://www.navy.gov.au>

✓ Following

Tweets Favorites Following Followers Lists

Australian_Navy Navy Webmaster
News: Pacific Partnership 2011 comes to an end
<http://goo.gl/fb/6c9bb>
20 Jul

Australian_Navy Navy Webmaster
News: Navy to Set Sail for Subantarctic Wilderness
<http://goo.gl/fb/A8CpJ>
19 Jul

Australian_Navy Navy Webmaster
News: Balikpapan lends a hand <http://goo.gl/fb/2Yfll>
17 Jul

Australian_Navy Navy Webmaster
News: The Sea Kings and EOD's <http://goo.gl/fb/ss8tx>
15 Jul

Australian_Navy Navy Webmaster
News: HMAS Stirling Time Capsule <http://goo.gl/fb/Knulv>
15 Jul

Australian_Navy Navy Webmaster
News: Centenary of the Royal assent of the Australian Navy
<http://goo.gl/fb/sCqaN>
11 Jul

Australian_Navy Navy Webmaster
News: Navy Celebrates 100 Years and invites Darwin to the party
<http://goo.gl/fb/ktkrQ>
11 Jul

Australian_Navy Navy Webmaster
News: Northern Territory Police, Fire and Emergency Services sign

Screenshot, 22 July 2011

Features:

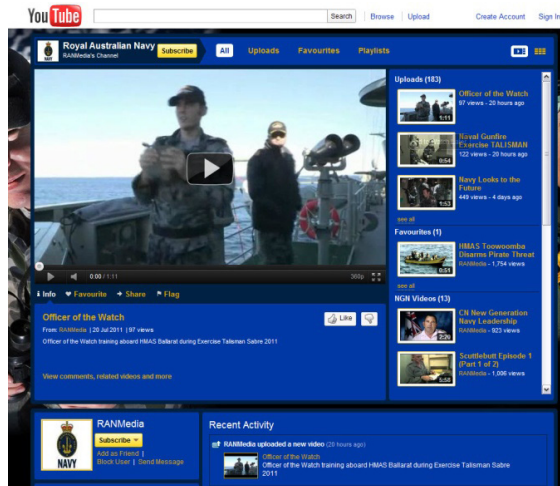
- Official account.
- Does not appear to interact much with other Twitter users.
- Used as a broadcast medium for news.
- Using goo.gl shortened URLs for tracking click-throughs.

YouTube

Royal Australian Navy

Channel views – 20,044
Total upload views – 167,260
Subscribers – 331

[www.youtube.com/
user/RANmedia](http://www.youtube.com/user/RANmedia)



Screenshot, 22 July 2011

Features:

- Official account.
- Includes a disclaimer regarding advertising or promoted videos.

Note: Embedded YouTube players include links to and advertising of other videos at the conclusion of each video's content, this 'banner' of content represents advertising on the part of YouTube and cannot be controlled or removed by us. It may include irrelevant, inappropriate and potentially offensive video clips.

- Updated frequently.
- Comments enabled on videos
- limited comments that are generally positive
- either the account is well monitored or the content is not controversial enough to provoke argument.

**HMAS Melbourne
Association**

Channel views – 360
Total Upload views – 9,224
Subscribers – 2

www.youtube.com/user/hmasmelbourneassn



Screenshot, 22 July 2011

Features:

- Limited video content.
 - Last updated two years ago.
 - Comments enabled on videos.
 - Only very few comments on videos.
- Those are positive.

2.3.3 Australian Army

The audit for the Australian Army covered its presences on Facebook (pages and groups), Twitter, Flickr and YouTube.

Facebook (pages)

Australian Army

141,804 likes

**[www.facebook.com/
TheAustralianArmy](http://www.facebook.com/TheAustralianArmy)**



Screenshot, 21 July 2011

Features:

- Posting video from defence.gov.au site.
- Signing off as person for posts.
- Responding to questions.
- Live Facebook chat for Army Challenge award.
- Posting images of maps, old weapons, people.

Possible improvements:

- Could do with more soldier images – making the brand personal.
- Need to improve the technical implementation of custom content pages.
- Need to be mindful of overposting – 11 posts in one day on 20 July 2011.
- Consider removing the ability for people to upload photos, or monitor uploads heavily – one image of a female has been uploaded, encouraging others to 'friend' her.

Facebook (pages)

9 RQR

1,526 likes

[www.facebook.com/
AustralianArmy9RQR](http://www.facebook.com/AustralianArmy9RQR)



Screenshot, 21 July 2011

Features:

- Page for reserves battalion.
- Posting photos.
- Responding to posts from old serving members and requests regarding recruitment.
- Page to promote battalion and keep family and friends happy.

Defence Townsville
'An official Australian
Army page'

363 likes

[www.facebook.com/
pages/Defence-Townsville/208359662515275](http://www.facebook.com/pages/Defence-Townsville/208359662515275)



Screenshot, 21 July 2011

Features:

- Does not appear to be an official page.
- States that it is an official Australian Army page.
- Not monitoring page for unrelated posts from users.
- Responding to user questions.
- 3 Brigade Townsville 'Face Book website'.
- Guidelines on what should/should not be on the Facebook page (in the info tab) are far too long.
- Contact for the guidelines is army.socialmedia@defence.gov.au.
- Posting photos, updates.

Facebook (pages)

**Australian Defence
Force: RAAMC
(Royal Australian
Army Medical Corps)**

453 likes

[www.facebook.com/
pages/Australian-
Defence-Force-
RAAMC/336556396341](http://www.facebook.com/pages/Australian-Defence-Force-RAAMC/336556396341)



Screenshot, 21 July 2011

Features:

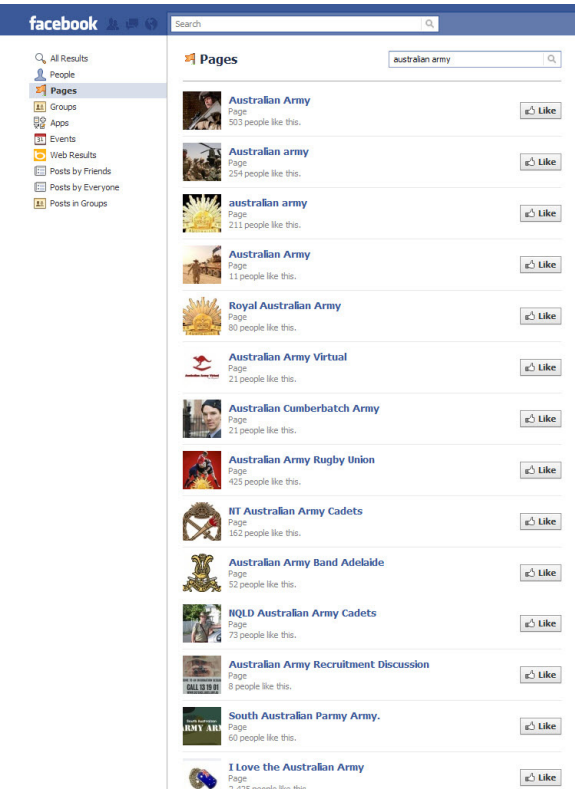
- Posts commemorating soldiers who have been killed.
- At 21 July 2011, last four posts were commemorating lost soldiers – affects the tone of the page.
- Posts photos.
- Users want to know who runs the page and the purpose.

Topic: Who is running this page?

Displaying all 14 posts.

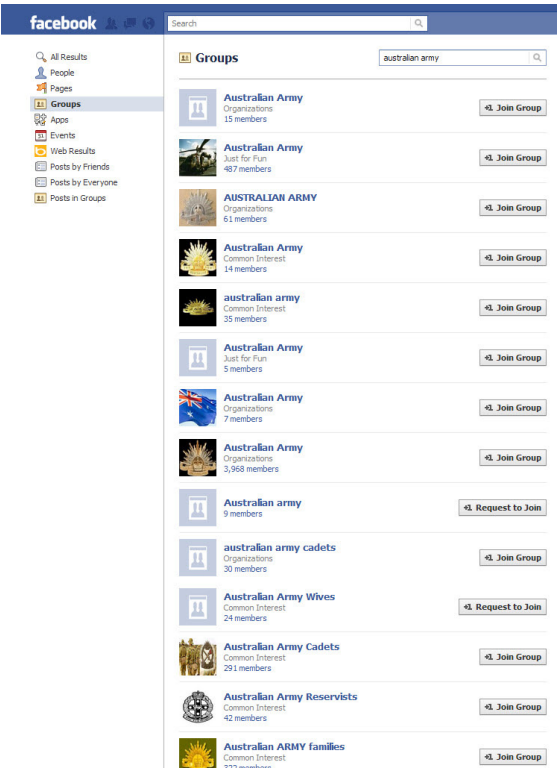
- Kane Bowden**
If the page creator could let themselves be known that would be great so we can get an idea of what the main purpose of this page is for. Pics, information for prospective medics, catch up with old friends etc. If so then we need some way to upload pics into albums and get more info on here besides a link to the defence intranet RAAMC site. Thanks.
over a year ago · Report
- Kane Bowden**
I guess the page fairies are running it then. Thanks guys and dolls.
over a year ago · Report
- Clara Brown**
Hello Page fairies, what Kane says is true. It would be great if everyone was able to upload photos and add info. There are a lot of people interested in this page that are joining up and could learn a great deal from your stories and experiences and those of other people on this page.
over a year ago · Report
- Australian Defence Force: RAAMC**
Hey sorry Kane I've been away for a while doing military exercises and haven't had time to be on the computer let alone Facebook. But yes this page is for Pictures, Information for prospective medics and of course catch up with old friends and even make new ones. So I'll get onto my 'Page Fairy' business straight away.
over a year ago · Report

A number of unofficial Australian Army pages appear in the Facebook search results, alongside official pages. The following image shows the Facebook search results.



Facebook (groups)

There are a number of unofficial Facebook groups with varying levels of Facebook security. Some of them are the older style, which resembles pages, and are soon to be archived.



Twitter

@Australian Army
(The Australian
Army)

3,211 followers
24 following
1,510 tweets

[http://twitter.com/#!/Aus-
tralianArmy](http://twitter.com/#!/AustralianArmy)



The Australian Army

@AustralianArmy Canberra, Australia
Official Australian Army Twitter: news, images from
army.gov.au (Following does not = Army Endorsement.)
<http://www.army.gov.au>

[Follow](#) [Text follow AustralianArmy to your carrier's shortcode](#)

[Tweets](#) [Favorites](#) [Following](#) [Followers](#) [Lists](#)

**AustralianArmy** The Australian Army
#FF @AirForceHQ @Australian_Navy @AWMemorial
26 minutes ago

**AustralianArmy** The Australian Army
Good choice mate! Check out <http://bit.ly/opgRq4> for info! Good luck
;) RT @katee_sarah: I'm doin it... I'm joining the @AustralianArmy!!
29 minutes ago

**AustralianArmy** The Australian Army
Great photos of 6RAR! RT @TalismanSabre: I posted 11 photos on
Facebook in the album "6th Battalion RAR" <http://bit.ly/pvOasC>
17 hours ago

**TalismanSabre** TalismanSabre [by AustralianArmy](#)
I posted 9 photos on Facebook in the album "Paratroopers"
<http://fb.me/RQZBgjHr>
18 hours ago

**AustralianArmy** The Australian Army
The Hon Warren Snowden today announced the launch of new
Alumni website for ex @Australian_Navy , Army and @AirForceHQ
<http://bit.ly/pdB7dX>
19 hours ago

**AustralianArmy** The Australian Army
The Australian Army's Captain Oldaker shows his US opponent who
has the upper hand @TalismanSabre <http://on.fb.me/oV23z9>
22 hours ago

**AustralianArmy** The Australian Army
Check out great images from Talisman Sabre! RT
@TalismanSabre: FB album "National Guard/Aus Army Reserve/1-
158 Cavalry" <http://bit.ly/qo61sy>
22 hours ago

Screenshot, 21 July 2011

Features:

- Official channel.
- Little evidence of direct response to mentions of @AustralianArmy.
- Retweeting and adding to tweets about joining the Army.



AustralianArmy The Australian Army
Good choice mate! Check out <http://bit.ly/opgRq4> for info! Good luck
;) RT @katee_sarah: I'm doin it... I'm joining the @AustralianArmy!!
29 minutes ago

- Disclaimer in account description says that following does not imply endorsement from the Australian Army.



The Australian Army

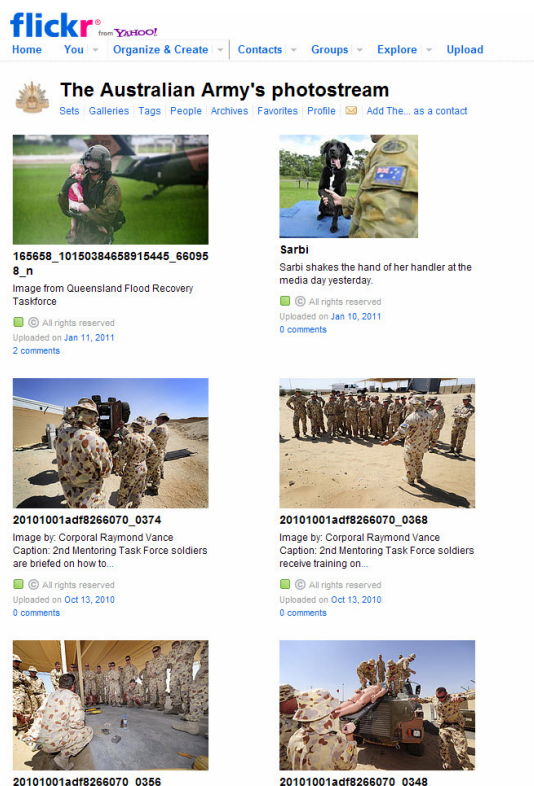
@AustralianArmy Canberra, Australia
Official Australian Army Twitter: news, images from
army.gov.au (Following does not = Army Endorsement.)
<http://www.army.gov.au>

Flickr

The Australian Army

Joined March 2010
190 items on Flickr

[www.flickr.com/photos/
AustralianArmy](http://www.flickr.com/photos/AustralianArmy/)



Screenshot, 21 July 2011

Features:

- Official account.
- Has not been updated since 11 January 2011.
- Examples of photo content
 - Queensland floods recovery taskforce
 - training
 - Dili patrol
 - East Timor deployments.
- Photos uploaded with filename should be renamed to reflect the subject of the image.

YouTube

206 Army Cadet Unit

Channel views – 897
Total upload views – 12,201
Subscribers – 21

[www.youtube.com/
user/206armycadetunit](http://www.youtube.com/user/206armycadetunit)



Screenshot, 21 July 2011

Features:

- Unclear whether this is official or unofficial.
- Lists school – Marist College.
- Examples of video content
 - recruit information
 - new intake of cadets
 - parade – officer cadets.
- Comments on some videos are inappropriate; requires monitoring.

2.3.4 Royal Australian Air Force

The audit for the RAAF covered its presences in Facebook (pages and groups), Twitter and YouTube.

Facebook (pages)

Royal Australian Air
Force

10,928 likes

[www.facebook.com/
RoyalAustralianAir-
Force](http://www.facebook.com/RoyalAustralianAirForce)



Screenshot, 20, July 2011

Features:

- Posting photos, YouTube videos, news articles.
- Responding to questions from the public.
- Message about social media posting for Defence personnel.

About

Defence personnel should read DI(G)ADMIN 08-1 before posting anything on social networking sites such as facebook.
<http://www.airforce.gov.au/images/FacebookPRF2.pdf>
<http://www.airforce.gov.au/images/security-poster.pdf>

- Security content page for service members.
- Had work experience person doing the updates for this page.



The following Facebook pages were listed on the official RAAF Facebook page as Facebook Fan pages. These pages (with the exception of I LOVE JET NOISE!) identify themselves as official pages for the RAAF and provide direction that Defence personnel must read DI (G) ADMIN 08-01 before posting in social media. Most of the pages have a 'Security' page with broken links. The pages promote content such as videos, photos and stories pertaining to the individual interests of the page and are used to promote official RAAF Facebook page events and the official RAAF Twitter account. Information retrieved on 21 July 2011.

Facebook fan page	Number of likes	Link to page	Features
Royal Australian Air Force Band >>Air Force Band<<	130 likes	http://www.facebook.com/AirForceBand	<ul style="list-style-type: none"> • Updates once every 1–2 months. • Limited number of photos.
I LOVE JET NOISE! (RAAF)	3,904 likes	http://www.facebook.com/ilovejetnoise	<ul style="list-style-type: none"> • Appears unofficial. • Posts content on planes or flying (photos, videos etc.). • Unclear who this page is run by. • Positive 'vibe' based on user interaction.
Royal Australian Air Force >>Balloon<<	153 likes	http://www.facebook.com/RAAF.Balloon	<ul style="list-style-type: none"> • Updated approximately once a month. • Posting photos of the balloon. • Limited interaction from users with posts.
Royal Australian Air Force B737-BBJ >>BBJ<<	264 likes	https://www.facebook.com/RAAF.BBJ	<ul style="list-style-type: none"> • Reasonable interaction from users, given the number of likes. • Updated approximately four times over six months.
Royal Australian Air Force PMVT >>Bushmaster<<	230 likes	http://www.facebook.com/RAAF.Bushmaster	<ul style="list-style-type: none"> • Currently updated once every 1–2 weeks. • Posts photos of Bushmaster vehicle.
Royal Australian Air Force C-130 >>Hercules<<	1,059 likes	http://www.facebook.com/RAAF.C130	<ul style="list-style-type: none"> • Posting YouTube videos, links to external sites and images. • Reasonable interaction from users, given the number of likes. • Includes a number of user-submitted photos.

Facebook fan page	Number of likes	Link to page	Features
Royal Australian Air Force C-17A >>Globemaster III<<	734 likes	http://www.facebook.com/RAAF.C17	<ul style="list-style-type: none"> • Updates at least once per week. • Posting links to external sites and images. • Includes a number of user-submitted photos.
Royal Australian Air Force CL-604 >>Challenger<<	224 likes	http://www.facebook.com/RAAF.Challenger	<ul style="list-style-type: none"> • Posting is sporadic and appears unplanned. • Posting links to external sites and images. • Reasonable interaction from users, given the number of likes.
Royal Australian Air Force DHC-4 >>Caribou<<	468 likes	http://www.facebook.com/RAAF.DHC4	<ul style="list-style-type: none"> • Reasonable interaction from users, given the number of likes. • Users post their own content on the page.
Royal Australian Air Force – F1-111 Jet >>Pig<<	3,904 likes	http://www.facebook.com/RAAF.F111	<ul style="list-style-type: none"> • Updating roughly every few days. • Posting videos and photos. • Reasonable interaction from users, given the number of likes.
Royal Australian Air Force F-35 >>JSF<<	906 likes	http://www.facebook.com/RAAF.F35	<ul style="list-style-type: none"> • Updating every couple of days. • Posting photos with accompanying stories or descriptions, videos and links to external sites. • Responds to posts from users, even if simply to say 'Thanks for sharing.'

Facebook fan page	Number of likes	Link to page	Features
Royal Australian Air Force Hawk 127 >>Hawk<<	403 likes	http://www.facebook.com/RAAF.Hawk	<ul style="list-style-type: none"> • Posting photos and links. • Reasonable interaction from users, given the number of likes.
Royal Australian Air Force F/A-18 >>Hornet<<	1,399 likes	http://www.facebook.com/RAAF.Hornet	<ul style="list-style-type: none"> • Updating every few days. • Posting photos, YouTube videos and links to external sites. • Reasonable interaction from users, given the number of likes.
Royal Australian Air Force KC-30A >>MRTT<<	338 likes	http://www.facebook.com/RAAF.KC30A	<ul style="list-style-type: none"> • Updating roughly once a week. • Posting photos, YouTube videos and links to external sites. • Reasonable interaction from users, given the number of likes.
Royal Australian Air Force K350 >>King Air<<	170 likes	http://www.facebook.com/RAAF.KingAir	<ul style="list-style-type: none"> • Last updated in June 2011, and before that in March 2011. • Limited interaction from users with posts. • Posting photos and videos. • Limited photo content.
Royal Australian Air Force AP-3C >>Orion<<	734 likes	http://www.facebook.com/RAAF.Orion	<ul style="list-style-type: none"> • Updating a few times a month. • Posting photos, videos and links to external websites. • Reasonable interaction from users, given the number of likes.

Facebook fan page	Number of likes	Link to page	Features
Royal Australian Air Force Aerial Display Team >>Roulettes<<	1,003 likes	http://www.facebook.com/RAAF.Roulettes	<ul style="list-style-type: none"> • Updating a few times a month. • Posting photos, videos and links to external websites. • High levels of interaction from users through posting on the page. • Responding to or 'liking' user posts.
Royal Australian Air Force PC-9A >>Trainer<<	299 likes	http://www.facebook.com/RAAF.PC9	<ul style="list-style-type: none"> • Updating a few times a month. • Posting photos, videos and links to external websites. • Limited interaction from users through posts.
Royal Australian Air Force F/A-18F>>Super Hornet<<	1,463 likes	http://www.facebook.com/RAAF.Super-Hornet	<ul style="list-style-type: none"> • Updating at least once a week. • Posting photos, videos and links to external websites. • Reasonable interaction from users, given the number of likes.
Royal Australian Air Force B737 AEW&C >>Wedgetail<<	485 likes	http://www.facebook.com/RAAF.Wedgetail	<ul style="list-style-type: none"> • Posting photos, videos and links to external websites. • Reasonable interaction from users, given the number of likes. • Responds to posts from users, even if simply to say 'Thanks for sharing.'

A number of other Facebook pages claim to represent the RAAF, but whether they are official or unofficial is not clear. Based on the number of ‘likes’ for these pages (some shown below), it is reasonable to infer that these pages have either been created recently or are unofficial.

	Royal Australian Air Force Ensign Page 6 people like this.	
	Royal Australian Air Force Aircraft Page 5 people like this.	
	Royal Australian Air Force Academy Page 2 people like this.	
	Royal Australian Air Force Memorial Page 2 people like this.	
	Royal Australian Air Force air marshals Page 3 people like this.	
	Royal Australian Air Force bases Page 3 people like this.	
	Royal Australian Air Force officers Page 2 people like this.	
	Royal Australian Air Force airmen Page 2 people like this.	
	The Royal Australian Air Force 22289 Exploration Dr, Lexington Park, MD 20653-2062 2 people like this. 0 check-ins.	
	Royal Australian Air Force cricketers Page 1 person likes this.	
	Royal Australian Air Force Maritime Section Page 4 people like this.	
	Dept. of Defence, Royal Australian Air Force Page 2 people like this.	
	Women's Royal Australian Air Force Page 4 people like this.	
	History of the Royal Australian Air Force Page 7 people like this.	
	List of Royal Australian Air Force installations Page 3 people like this.	

Facebook (groups)

There are a number of unofficial Facebook groups with varying levels of Facebook security. Some of them are the older style, which resembles pages, and are soon to be archived by Facebook.

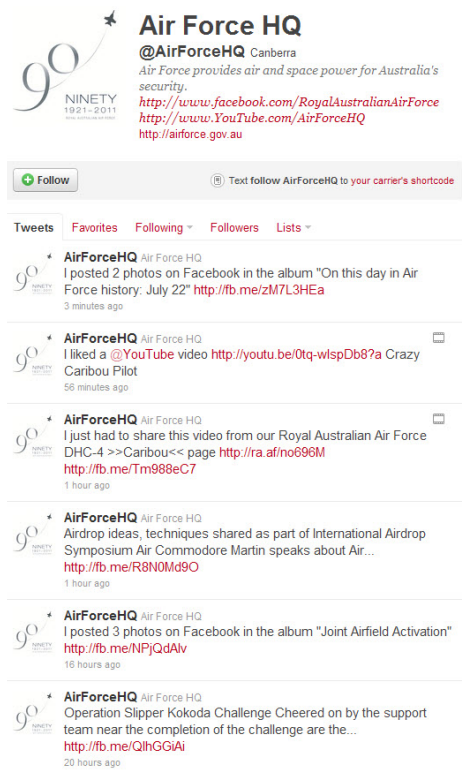
facebook			Search
All Results			Groups
People			raaf
Pages			
Groups			
Apps			
Events			
Web Results			
Posts by Friends			
Posts by Everyone			
Posts in Groups			
RAAF			Join Group
RAAF			Request to Join
RAAF			Request to Join
RAAF Townsville			Request to Join
RAAF medicos			Join Group
RAAF GAIK			Join Group
RAAF School			Request to Join
The RAAF			Join Group
RAAF Movements			Request to Join
RAAF Brats			Join Group
RAAF Darwin			Request to Join
RAAF STS			Request to Join
RAAF brats			Join Group
Raaf devil			Request to Join

Twitter

@AirForceHQ
(Air Force HQ)

1,216 followers
198 following
3,169 tweets

<http://twitter.com/#!/airforcehq>



Screenshot, 22 July 2011

Features:

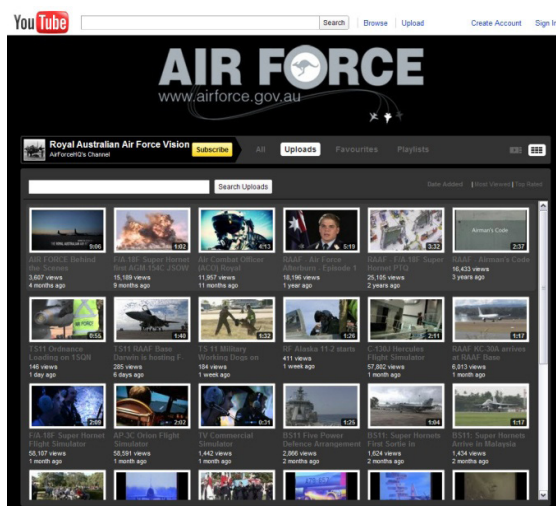
- Official account.
- Facebook and YouTube accounts linked to show activity.
- Does not appear to interact much with other Twitter users.
- Most tweets about promoting Facebook or YouTube accounts.
- Used for broadcast.

YouTube

Air Force HQ

Channel views – 83,334
Total upload views – 766,597
Subscribers – 1,227

www.youtube.com/user/AirForceHQ



Screenshot, 22 July 2011

Features:

- Official account.
- Comments enabled on videos.
- Video comments are generally positive.
- Videos are professional.
- Channel description promotes other official social media sites of the RAAF.

GLOSSARY AND REFERENCES

Glossary

API (application programming interface)	A set of rules, guides and code that can be used by developers to build software (such as apps and plugins).
Apps	Software applications with specific uses, often on a mobile phone or within another software platform, such as Facebook.
Defence	The Australian Defence Force, its component Services and the Department of Defence.
EOP (external official presence)	An officially approved and managed presence in a social media site or service (US).
Facebook	An integrated online social network that is currently the most commonly used in Australia and elsewhere.
Facebook Connect	A software platform that allows Facebook functionality to be integrated with and installed on other websites, so that users can engage with those websites using their Facebook login details.
Facebook lists	The grouping of Facebook friends into lists for the purpose of publishing specific content to those on the lists.
Facebook page	A location on Facebook to represent a company, brand, individual or community.
Facebook profile	A personal page representing a user's account and its elements, such as the user's settings and content (photos, videos and links).
Facebook wall	A space on a user's profile or page on which 'friends' or 'likers' can post content.
foursquare	Software service for mobile devices that allows users to 'check in' to a physical location using the geo-targeting functionality built into smart phones and mobile devices.
Friendster	A social gaming platform; widely acknowledged as the first integrated social network.
Google+	A new integrated social network, the beta version of which was launched in June 2011. The network is not yet open to everyone and is available by invitation only.
Google+ circles	Similar to Facebook lists, circles within Google+ allow users to be grouped so that content can be shared with those in the circle.
hashtag	A Twitter concept where short words or phrases preceded by a hash sign allow topics to be grouped and searched.
Like	A Facebook button or link present on all content posted to Facebook, or integrated into websites via Facebook Connect, which allows individuals to 'like' a piece of content. This information is gathered by Facebook and used to present targeted advertising to users.
LinkedIn	A social network where professionals can create profiles, add employment information and connect to other professionals.
logins	Details such as an email and password required to access a secure site, collectively referred to as 'logins'.

Myspace	Recognised as the first integrated social network; now overtaken by Facebook but still among the highest traffic sites in Australia.
netiquette	Internet etiquette; social conventions for communicating on the internet.
phishing	Posing as a legitimate entity to fraudulently collecting the personal information of online account holders.
plugin	An extension to a piece of software.
Recommend	Similarly to Facebook 'Likes', 'Recommends' are used through Facebook Connect by websites, such as news services, which publish content that may be inappropriate to 'like'.
Screenshot	Using the 'print screen' button on a computer keyboard to capture an image of the content on the monitor at the time.
Share	To pass content from one web user to another using functionality provided by the software hosting the content.
searchable web	All online content that is not contained within secure social media, such as individuals' profiles, and is therefore discoverable using a search engine.
Second Life	An online virtual world where individuals create 'avatars' (virtual characters) to interact with each other in various virtual locations.
sentiment	The positive or negative tone directed towards a brand or subject; used in social media monitoring.
smartphone	A mobile phone that offers features such as internet access, GPS and other technology that is not included in basic phones.
social network sites	Web-based services (such as Facebook and Myspace) that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. Users can connect by creating personal information profiles and inviting friends and colleagues to access their profile, send emails and instant messages. Profiles usually include photographs, videos, audio files, blogs and so on.
social web	The areas of the web that mainly involve interactions between individuals.
tablet	Hardware that is in between mobile phones and laptop computers in size and functionality.
tagging (photos)	Selecting a section of a photo and connecting it with the profile of the individual in the photo.
trolls	Online social media users (usually anonymous) who post controversial or aggressive messages for the purpose of causing offence or baiting others into arguments.
tweet	A status update through Twitter that can be up to 140 characters long; the act of sending a Twitter status update.

UCMJ (Uniform Code of Military Justice)	The foundation of US military law, exercising the authority of the US Constitution.
UGC (user-generated content)	Various forms of media content created by and available to users of social media.
viral	Adjective referring to the rapid and wide circulation of a piece of content on the internet.
Web 1.0	The initial phase of the internet, which involved the publishing of websites to domains and ecommerce, with limited user-generated content and interaction.
Web 2.0	A subsequent stage in the evolution of the internet, which allows users to generate content, publish it, and interact with others' content.
widget	A piece of functionality within an application, such as a chat widget within the Facebook application on a mobile phone.
WordPress	Open source blog software that can be hosted by a third party or custom installed.

Abbreviations and acronyms

ACCC	Australian Competition and Consumer Commission
ACL	Australian Consumer Law
ACMA	Australian Communications and Media Authority
ADF	Australian Defence Force.
ADFA	Australian Defence Force Academy.
ALRC	Australian Law Reform Commission
API	application programming interface
APPs	Australian Privacy Principles
BAV	<i>BrandAsset Valuator</i>
BCC	Brisbane City Council (Queensland, Australia)
CNO	Chief Naval Officer (US)
DEOC	Digital Executive Oversight Committee (proposed)
DRN	Defence Restricted Network
DSN	Defence Secret Network
EIDWS	enlisted information dominance warfare specialist (US)
EOP	External Official Presence (US)
EOP	electronic online presence
FRGs	family readiness groups (US)
ICT	information and communications technology
IDC	Information Domination Corps (US)
KPI	key performance indicator
NMITC	Navy and Marine Intelligence Training Center (US)
NPPs	National Privacy Principles
OPSEC	operational security
ORM	operational risk management
QPS	Queensland Police Service.
PR	public relations
RAAF	Royal Australian Air Force
RAN	Royal Australian Navy
SMS	short message service
SOPs	standard operating procedures
UCMJ	Uniform Code of Military Justice (US)
UGC	user-generated content
US DOD	United States Department of Defense

References

Overview

Department of Defence (Australian Government), 2011, 'Reviews into the Australian Defence Force Academy, the Australian Defence Force and Defence culture'. Retrieved 4 July 2011 from <http://www.minister.defence.gov.au/2011/05/06/reviews-into-the-australian-defence-force-academy-the-australian-defence-force-and-defence-culture/>

Section 1 – Social media and their origins

ABC (Australian Broadcasting Corporation) 2011, *Technology explained – social media*. Retrieved 12 July 2011 from <http://www.abc.net.au/technology/techexplained/articles/2011/04/11/3158241.htm>.

Ackerman S 2011, 'Marines boot social media pioneers from Afghanistan Facebook freakout'. Retrieved 8 July 2011 from <http://www.wired.com/dangerroom/2011/03/marines-boot-social-media/>.

Bewley TF 1999, *Why wages don't fall in a recession*, Harvard University Press, Cambridge, MA.

Bronk C 2009, 'Marines' social-media ban is bad for morale', *Federal Computer Week*. Retrieved 8 July 2011 from <http://fcw.com/articles/2009/09/21/comment-chris-bronk-marine-ban.aspx>.

Dwyer, D. 2009, *Communications in Business: Strategies and Skills*, Pearson Education Australia, Frenchs Forest, NSW.

Ferraro GP 2002, *The cultural dimension of international behavior*, Pearson Education, Upper Saddle River, New Jersey.

Hall, E.T. & Hall, M.R. 1990, *Understanding Cultural Differences*, Intercultural Press, Yarmouth ME, USA.

Hill CWL 2003, *International business: competing in the global marketplace*, Irwin, Chicago.

Hoebel EA & Frost EL 1976, *Cultural and social anthropology*, McGraw-Hill, New York.

Hofstede G 1984, *Culture's consequences: international differences in work-related values*, abridged edition, Sage Publications, Beverly Hills, CA.

Hofstede G 1991, *Culture and organisations*, McGraw-Hill, New York.

Jacka JM & Scott PR 2011, *Auditing social media – a governance and risk guide*, John Wiley and Sons, United States of America.

Jones ML 2007, 'Hofstede – Culturally questionable?', paper presented to the Oxford Business & Economics Conference, Oxford, 24–26 June. Retrieved 11 July 2011 from <http://ro.uow.edu.au/commpapers/370>.

Kaplan A & Haenlein M 2010, 'Users of the world, unite! The challenges and opportunities of social media', *Business Horizons*, vol. 53, pp. 59–68. Retrieved 11 July 2011 from the ScienceDirect database. doi:10.1016/j.bushor.2009.09.003.

Mead R 2005, *International management: cross-cultural dimensions*, 3rd edition, Blackwell USA.

Mwaura G, Sutton J & Roberts D 1998, 'Corporate and national culture – an irreconcilable dilemma for the hospitality manager?', *International Journal of Contemporary Hospitality Management*, vol. 10, no. 6, pp. 212–220. Retrieved 10 July 2011 from the Emerald Insight database.

Oxford Dictionary 2011a, Oxford Dictionaries, Oxford, UK. Retrieved 12 July 2011 from <http://oxforddictionaries.com/definition/social+media>.

Oxford Dictionary 2011b, Oxford Dictionaries, Oxford, UK. Retrieved 12 July 2011 from <http://oxforddictionaries.com/definition/social+networking>.

Peterson M 2007, 'The heritage of cross cultural management research: implications for the Hofstede Chair in Cultural Diversity', *International Journal of Cross Cultural Management*, vol. 7, no. 3, pp. 359–377. Retrieved 11 July 2011 from the Sage Journals Online.

Samovar LA & Porter RE 1991, *Communication between cultures*, 3rd edn, Wadsworth, California.

The Social Media Guide 2011, '50 definitions of social media'. Retrieved 12 July 2011 from http://thesocialmediaguide.com/social_media/50-definitions-of-social-media

Section 2.1 – Trends

ABC (Australian Broadcasting Corporation) 2011, 'Facebook under fire for photo tagging feature'. Retrieved 18 July 2011 from <http://www.abc.net.au/news/2011-06-09/facebook-under-fire-for-photo-tagging-feature/2753000?section=justin>

Australian Bureau of Statistics 2011, 'Australian demographic statistics, Dec 2010'. Retrieved 21 July 2011 from <http://www.abs.gov.au/ausstats/abs@.nsf/mf/3101.0>

ACMA (Australian Communications and Media Authority) 2011, 'The internet service market and Australians in the online environment'. Retrieved 13 July 2011 from http://www.acma.gov.au/webwr/assets/main/lib310665/the_internet_service_market_in_australia.pdf

Berkun S 2011, 'Post comments using Twitter and Facebook'. Retrieved 18 July 2011 from <http://en.blog.wordpress.com/2011/06/07/post-comments-twitter-facebook/>

Boyd D & Ellison N 2008, 'Social network sites: definition, history, and scholarship', *Journal of Computer-Mediated Communication*, vol. 13, pp. 210–230. Retrieved 11 July 2011 from the Wiley Online Library at <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full>.

CBR Communications Mobility 2011, 'Australia and New Zealand media tablet markets to double in 2011: IDC'. Retrieved 13 Jul 2011 from <http://mobility.cbronline.com/news/australia-and-new-zealand-media-tablet-markets-to-double-in-2011-idc-290611>

CNET Australia 2011, 'Apple first in Aussie phone market: IDC'. Retrieved 13 July 2011 from <http://www.cnet.com.au/apple-first-in-aussie-phone-market-idc-339317492.htm>

Colgan P, Vaughan O & Davidson H 2011, 'Cyclone Yasi: how it unfolded'. Retrieved 17 July 2011 from <http://www.news.com.au/breaking-news/floodrelief/north-queensland-braces-for-cyclone-anthony-as-cyclone-yasi-breeds-behind-it/story-fn7ik2te-1225998711771>

comScore 2011, 'Social networking accounts for 1 in every 5 minutes spent online in Australia'. Retrieved 13 July 2011 from http://www.comscore.com/Press_Events/Press_Releases/2011/2/Social_Networking_Accounts_for_1_of_Every_5_Minutes_Spent_Online_in_Australia

comScore 2010, 'Facebook and Twitter access via mobile browser grows by triple-digits in the past year'. Retrieved 13 July 2011 from http://www.comscore.com/Press_Events/Press_Releases/2010/3/Facebook_and_Twitter_Access_via_Mobile_Browser_Grows_by_Triple-Digits

Daily Telegraph 2009, 'Jeff Goldblum watches Richard Wilkins reporting his death'. Retrieved 20 July 2011 from <http://www.dailytelegraph.com.au/entertainment/jeff-goldblum-watches-richard-wilkins-reporting-his-death/story-e6frewyr-1225744887122>

Elowitz B 2011, 'The web is shrinking. Now what?' Retrieved 18 July 2011 from <http://allthingsd.com/20110623/the-web-is-shrinking-now-what/?mod=sn>

Facebook 2011, 'Create an ad'. Retrieved 21 July 2011 from https://www.facebook.com/ads/create/?src=emu1&campaign_id=282141474901&placement=emuca&extra_1=0

Facebook developers 2011, 'Graph API'. Retrieved 25 July 2011 from <http://developers.facebook.com/docs/reference/api/>

Games Blog 2011, 'Angry Birds cheats and tips: 'Like' it on Facebook, win three free levels'. Retrieved 19 July 2011 from <http://blog.games.com/2011/07/11/angry-birds-cheats-tips-facebook-free-levels/>

Gizmodo 2010, 'The most popular iOS Apps of 2010'. Retrieved 13 July 2011 from <http://www.gizmodo.com.au/2010/12/the-most-popular-ios-apps-of-2010/>

HTC 2011, 'HTC ChaCha'. Retrieved 19 July 2011 from <http://www.htc.com/www/product/chacha/specification.html>

Hutchings E 2011, 'Foursquare partners with daily deals companies'. Retrieved 25 July 2011 from <http://www.psfk.com/2011/07/foursquare-partners-with-daily-deals-companies.html>

Larkin T 2011, 'Social media earns its stripes in disaster communication'. Retrieved 17 July 2011 from http://www.police.qld.gov.au/Resources/Internet/services/reportsPublications/bulletin/357/documents/357_p36-37_socialmedia1.pdf

Lee J 2010, '10 million Aussies in love with Facebook', *The Sydney Morning Herald*, 10 December 2010. Retrieved 18 July 2011 from <http://www.smh.com.au/small-business/smallbiz-marketing/10-million-aussies-in-love-with-facebook-20101210-18s05.html>

Mashable 2011, 'How social media's short news cycle can precipitate bad journalism'. Retrieved 20 July 2011 from <http://mashable.com/2011/06/15/social-media-news-cycle-journalism/>

Net Marketing Strategies 2010, 'Social Media & Marketing Daily: mobile social activity on the rise'. Retrieved 19 July 2011 from <http://net-marketing-strategies.com/social-media-marketing-daily-mobile-social-activity-on-the-rise/>

Newsphobia 2009, 'Richard Wilkins – international butt of the joke', *The Daily Telegraph*. Retrieved 20 July 2011 from <http://www.dailytelegraph.com.au/entertainment/jeff-goldblum-watches-richard-wilkins-reporting-his-death/story-e6frewyr-12257448871222>

The Nielsen Company 2011, 'Led by Facebook, Twitter, global time spent on social media sites up 82% year over year'. Retrieved 13 July 2011 from <http://blog.nielsen.com/nielsenwire/global/led-by-facebook-twitter-global-time-spent-on-social-media-sites-up-82-year-over-year/>

QuickerFeet 2011, 'The QuickerFeet iPhone app'. Retrieved 18 July 2011 from <http://www.quickerfeet.com/>

Reuters 2011, 'Reporting from the internet and using social media'. Retrieved 20 July 2011 from http://handbook.reuters.com/index.php/Reporting_from_the_internet

Schroeder S 2011, 'Facebook's automated photo tagging prompts EU probe'. Retrieved 18 July 2011 from <http://mashable.com/2011/06/08/facebook-eu-probe/#>

Sensis 2011, 'Social media report: what Australian people and businesses are doing with social media'. Retrieved 13 July 2011 from [http://about.sensis.com.au/IgnitionSuite/uploads/docs/SENSIS%20SOCIAL%20MEDIA%20REPORT\[2\].pdf](http://about.sensis.com.au/IgnitionSuite/uploads/docs/SENSIS%20SOCIAL%20MEDIA%20REPORT[2].pdf)

Solis B 2011, 'Google will not run circles around Facebook, but it gets a +1'. Retrieved 20 July 2011 from <http://www.fastcompany.com/1767988/google-will-not-run-circles-around-facebook-but-it-gets-a-1>

Telstra 2011, 'Tribe'. Retrieved 19 July 2011 from <http://www.telstra.com.au/mobile/services/socialnetworking/tribe.html>

Tsotsis A 2011, 'Sean Parker on why Myspace lost to Facebook'. Retrieved 18 July 2011 from <http://techcrunch.com/2011/06/28/sean-parker-on-why-myspace-lost-to-facebook/>

Twitpic 2011, 'Dan Nolan: Oh my god this just washed up in Gympie (via a mate)'. Retrieved 20 July 2011 from <http://twitpic.com/3p21ze>

Vodafone 2011, 'Mobile phone plans, caps and contracts – Vodafone Australia'. Retrieved 19 July 2011 from <http://www.vodafone.com.au/personal/plans/>

Section 3.1.1 – Management – international best practice

Air University 1950, 'Uniform Code of Military Justice'. Retrieved 30 June 2011 from <http://www.au.af.mil/au/awc/awcgate/awc-law.htm#ucmj>

BMD (British Ministry of Defence) 2011a, 'Friends and family'. Retrieved 15 June 2011 from <http://www.blogs.mod.uk/onlinesecurity/family.html>

BMD (British Ministry of Defence) 2011b, 'What to do if something goes wrong', *Personal Safety Online*. Retrieved 20 July 2011 from <http://www.blogs.mod.uk/onlinesecurity/wrong.htm>

Canadian Forces 2011, 'Web site terms and conditions of use'. Retrieved 25 July 2011 from <http://myforces.ca/pg/xpages/read/terms>

Department of State 2009, 'Social networking cyber security awareness briefing'. Retrieved 26 July 2011 from <http://www.slideshare.net/DepartmentofDefense/social-media-cyber-security-awareness-briefing>

Dorsett J 2009a, 'Memorandum for the Information Dominance Corps – 17 December 2009'. Retrieved 25 July 2011 from <http://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjYxYjZiYmY4ODZkYmQyNzg>

Dorsett J 2009b, 'Memorandum for the Information Dominance Corps – 2 November 2009'. Retrieved 25 July 2011 from <http://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjI1MWFjYjZiNDhMjk3MzY>

Dorsett J 2010a, 'Note from the DCNO for Information Dominance – October 2010'. Retrieved 25 July 2011 from <http://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjJkMGQ3OGMxMzVhMWRINTQ>

Dorsett J 2010b, 'The Information Dominance Corps: what does it mean to me?'. Retrieved 25 July 2011 from <http://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjRjMTY5YWMxZjk5MTVhMjU>

Dorsett J 2010c, 'Talking with Vice Adm. Jack Dorsett'. Retrieved 25 July 2011 from <https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjUyZDc0NDM4OGQzY2MzMmM>

Dorsett J 2011a, 'DCNO for Information Dominance Update – April, 2011'. Retrieved 25 July 2011 from <http://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjUxZTM0OTBiZjUwY2FINWI>

Dorsett J 2011b, 'DCNO for Information Dominance Update – May 4, 2011'. Retrieved 25 July 2011 from [http://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjM4ZjE5Mml3NDU5ZmFiMTI; http://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjlyZjM4MzY1ZGFhNWQ3YjEE](http://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjM4ZjE5Mml3NDU5ZmFiMTI;http://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjlyZjM4MzY1ZGFhNWQ3YjEE)

Fabrizio E 2010, 'The dangers of friending strangers: the Robin Sage experiment'. Retrieved 14 July 2011 from <http://science.dodlive.mil/2010/07/21/the-dangers-of-friending-strangers-the-robin-sage-experiment/>

Leigher WE 2011, 'Learning to operate in cyberspace', *U.S. Naval Institute*. Retrieved 25 July 2011 from <http://www.usni.org/magazines/proceedings/2011-02/learning-operate-cyberspace>

McCullough BJ 2010, 'Statement of VADM J. McCullough III, Commander, United States Fleet Cyber Command, before the Terrorism and Unconventional Threats Capabilities Subcommittee of the House Armed Services Committee'. Retrieved 25 July 2011 from <http://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjY4MTk0OWUwMGVIZWUyMGYY>

McHugh JM 2009 'Delegation of authority – approval of external official presences', *US Army*. Retrieved 25 July from <http://www.slideshare.net/USArmySocialMedia/delegation-of-authority-social-media-use>

Meek TP 2010, 'COMNAVCYBERFOR INSTRUCTION 1414.1', Department of the Navy. Retrieved 25 July 2011 from <https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjlyZjM4MzY1ZGFhNWQ3YjE>

NARA (National Archives and Records Administration) 2010, 'A report on federal web 2.0 use and record value'. Retrieved 25 July 2011 from <http://www.archives.gov/records-mgmt/resources/web2.0-use.pdf>

OSPA (Operations Security Professional's Association) 2011, 'OPSEC for families'. Retrieved 21 July 2011 from <http://www.opsecprofessionals.org/training.html>

Parsons M 2010, 'The impact of new media on military operations', *Canadian Forces College*. Retrieved 25 July 2011 from http://www.cfc.forces.gc.ca/en/cfcpapers/index.php?keywords=n&start=1161&search_where=title&yearLimit=all&programLimit=all&submit=Search

Ryan T 2010, 'Getting in bed with Robin Sage'. Retrieved July 14 2011 from <https://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf>

Sullivan P & Kutch M 2009, 'SPAWAR Systems Center Pacific and Atlantic – cyber perspectives and strategy', NDIA San Diego Symposium, 26–28 October, National Defense Industrial Association – San Diego Chapter.

Upal A 2010, 'The role of narratives in shaping people's social identity beliefs', Defence R&D Canada, Toronto, April 2010. Retrieved 20 July from http://pubs.drdc.gc.ca/PDFS/unc104/p534365_A1b.pdf

US Air Force 2009, 'Social media and the Air Force'. Retrieved 26 July 2011 from <http://www.slideshare.net/DepartmentofDefense/air-force-new-media-manual>

US Army 2010a, 'Flickr strategy'. Retrieved 25 July 2011 from <http://www.slideshare.net/USArmySocialMedia/us-army-flickr-strategy>

US Army 2010b, 'Twitter strategy' Retrieved 25 July 2011 from <http://www.slideshare.net/USArmySocialMedia/us-army-twitter-strategy>

US Army 2010c, 'Social media strategies for military spouses and dependents'. Retrieved 26 July 2011 from <http://www.slideshare.net/USArmySocialMedia/frsa-frg-family-and-spouses-briefing>

US Army 2011, *The United States Army social media handbook*. Retrieved 20 July 2011 from <http://www.slideshare.net/USArmySocialMedia/army-social-media-handbook-2011>

US DOD (Department of Defense) 2010a, 'DoD Live! Communicating effectively using creative online strategies'. Retrieved 25 July 2011 from <http://www.slideshare.net/DepartmentofDefense/new-media-briefing>

US DOD (Department of Defense) 2010b, 'Getting started with blogging – a guide for creating official pages'. Retrieved 26 July 2011 from <http://www.slideshare.net/DepartmentofDefense/getting-started-with-blogs-4745932>

US Navy 2010a, 'US Navy's vision for information dominance'. Retrieved 25 July 2011 from <http://navintpro.net/wp-content/uploads/2010/06/Navy-Information-Dominance-Vision-May-2010.pdf>

US Navy 2010b, 'Information dominance and the U.S. Navy's cyber warfare vision'. Retrieved 25 July 2011 from <http://www.dtic.mil/ndia/2010SET/Dorsett.pdf>

US Navy 2010c, 'Social media snapshot – Operations Security (OPSEC)'. Retrieved 21 July 2011 from <http://www.slideshare.net/DepartmentofDefense/opsec-snapshot-4332606>

US Navy 2010d, 'Designation letter sample'. Retrieved 25 July 2011 from <http://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnpZGNzeW5jfGd4OjI2MTM5ZjJINjBiODY5M2Q>

US Navy 2010e, 'Navy Command social media handbook'. Retrieved 25 July 2011 from <http://www.slideshare.net/USNavySocialMedia/navy-command-social-media-handbook-web>

US Navy 2010f, 'Social media snapshot, Family Readiness Groups: researching family members through Facebook'. Retrieved 20 July 2011 from <http://www.slideshare.net/USNavySocialMedia/us-navy-family-readiness-groups-and-facebook>

US Navy 2010g, 'Social media snapshot – Operations Security (OPSEC)'. Retrieved 21 July 2011 from <http://www.slideshare.net/DepartmentofDefense/opsec-snapshot-4332606>

US Navy 2010h, 'Social media snapshot – applying operational risk management (ORM) principles to social media'. Retrieved 21 July 2011 from <http://www.slideshare.net/USNavySocialMedia/applying-operational-risk-assessment-orm-principles-to-social-media>

Sections 3.1.2 and 3.1.3 – Management – Defence practices and procedures / Discussion

DI(G) ADMIN 08-1 *Public comment and dissemination of official information by Defence personnel* (available on Defence intranet only).

Australian Government 2010, 'Government Response to the Report Government 2.0 Taskforce'. Retrieved 9 August 2011 from <http://www.finance.gov.au/publications/gov-response20report/doc/Government-Response-to-Gov-2-0-Report.pdf>

Jacka JM & Scott PR 2011, *Auditing social media – a governance and risk guide*, John Wiley and Sons, United States of America.

Mayfield TD 2011, 'A commander's strategy for social media', *Joint Forces Quarterly*, issue 60, 1st quarter 2011. Retrieved 16 July 2011 from <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA535374>

Prensky M 2001, 'Digital natives, digital immigrants', *On the Horizon*, vol. 9, no. 5, October. Retrieved 8 July from <http://www.marcprensky.com/writing/prensky%20-%20digital%20natives,%20digital%20immigrants%20-%20part1.pdf>

Section 3.2 – Morale

Ackerman S 2011, 'Marines boot social media pioneers from Afghanistan Facebook freakout'. Retrieved 8 July 2011 from <http://www.wired.com/dangerroom/2011/03/marines-boot-social-media/>.

Bewley TF 1999, *Why wages don't fall in a recession*, Harvard University Press, Cambridge, MA.

Bronk C 2009, 'Marines' social-media ban is bad for morale', *Federal Computer Week*. Retrieved 8 July 2011 from <http://fcw.com/articles/2009/09/21/comment-chris-bronk-marine-ban.aspx>.

Lanigan K 2008, 'Base services ease deployment stress', *VFW: Veterans of Foreign Wars Magazine*, vol. 95, no. 7, pp. 20–25. Retrieved 5 July 2011 from the Proquest Central database.

Levin A 2010, 'Military reviews all aspects of suicide-prevention efforts', *Psychiatric News*, vol. 45, no. 19, p. 6. Retrieved 5 July 2011 from <http://pn.psychiatryonline.org/content/45/19/6.2.short?rss=1>

Meyrowitz J 1985, *No sense of place: the impact of electronic media on social behaviour*, Oxford University Press, New York.

Rotter JC & Boveja ME 1999, 'Counseling military families', *The Family Journal*, vol. 7, no. 4, pp. 379–382. Retrieved 5 July 2011 from the Sage Journals Online.

US Army 2010a, *Five day social media strategy template*, United States Army, Washington DC. Retrieved 8 July from <http://www.slideshare.net/USArmySocialMedia/five-day-social-media-strategy-template-5532831>.

US Army 2010b, *Social media strategies for military spouses and dependents*, United States Army, Washington DC. Retrieved 8 July from <http://www.slideshare.net/USArmySocialMedia/frsa-frg-family-and-spouses-briefing>.

US Army 2011, *Social media handbook*, United States Army, Washington DC. Retrieved 8 July from <http://www.slideshare.net/USArmySocialMedia/army-social-media-handbook-2011>.

US DOD (Department of Defense) 2010, *The challenge and the promise: strengthening the force, preventing suicide and saving lives – final report of the Department of Defense Task Force on the Prevention of Suicide by Members of the Armed Forces*. Retrieved 8 July 2011 from <http://www.health.mil/dhb/downloads/Suicide%20Prevention%20Task%20Force%20final%20report%208-23-10.pdf>

USMC (United States Marine Corps) 2009, 'Immediate ban on internet social networking sites (SNS) on Marine Corps Enterprise Network (MCEN) NIPRNET'. Retrieved 8 July 2011 from <http://www.marines.mil/news/messages/pages/maradmin0458-09.aspx>

Weakliem DL & Frenkel SJ 2006, 'Morale and workplace performance', *Work and Occupations*, vol. 33, no. 3, pp. 335–361. Retrieved 5 July 2011 from the Emerald Insight database.

Wong W 2009, 'Is social media making you anti-social?', *Physorg.com*. Retrieved 8 July 2011 from <http://www.physorg.com/news162754989.html>

Section 3.3.1 – Marketing – international best practice

Blackburn J 2010, 'Veterans affairs – 2009–2010 departmental performance report'. Retrieved 26 July from <http://publications.gc.ca/site/eng/382991/publication.html>

BMD (British Ministry of Defence) 2011, 'Personal safety online'. Retrieved 20 July 2011 from <http://www.blogs.mod.uk/onlinesecurity/index.html>

Chang J 2010, 'Standardizing official U.S. Army external official presences (social media)', *US Army*. Retrieved 20 July 2011 from <http://www.slideshare.net/USArmySocialMedia/army-social-media-standard-operating-procedure-standardization>

Kyzer L 2011, 'Tip of the spear' (podcast), *Institute for Defense and Government Advancement*. Retrieved 20 July 2011 from http://www.idga.org/podcenter.cfm?category=government-transformation&title=social-media-and-the-military-with-lindy-kyzer&mac=IDGA_OI_Featured_2011&utm_source=idga.org&utm_medium=email&utm_campaign=HrOptIn&utm_content=7/5&TrackJoin=1

Long D 2011, 'Fake social media army used to sway public opinion', *Gizmodo*. Retrieved 20 July 2011 from <http://www.gizmodo.com.au/2011/03/fake-social-media-army-used-to-sway-public-opinion/>

McInay S 2010, 'Managing audience engagement to gain and retain public involvement', US Navy. Retrieved 20 July 2011 from <http://www.slideshare.net/USNavySocialMedia/managing-audience-engagement-to-gain-and-retain-public-involvement>

US Air Force 2009, 'Social media and the Air Force'. Retrieved 26 July 2011 from <http://www.slideshare.net/DepartmentofDefense/air-force-new-media-manual>

US Army 2010a, 'Facebook quick reference sheet – techniques learned from the very best pages'. Retrieved 20 July 2011 from <http://www.slideshare.net/USArmySocialMedia/facebook-handout-8029049>

US Army 2010b, 'Facebook strategy'. Retrieved 20 July 2011 from <http://www.slideshare.net/USArmySocialMedia/us-army-facebook-strategy>

US Army 2010c, 'Flickr strategy'. Retrieved 20 July 2011 from <http://www.slideshare.net/USArmySocialMedia/us-army-flickr-strategy>

US Army 2010d, 'Army social media best practices'. Retrieved 20 July 2011 from <http://www.slideshare.net/lindykyzer/army-social-media-best-practices-1310>

US Army 2011a, 'Social media roundup – 5 tips on how to effectively brand your social media presences'. Retrieved 20 July 2011 from <http://www.slideshare.net/thenatlguard/smr-week-22-social-media-branding-7616139>

US Army 2011b, 'Social media roundup – Personal conduct on social media platforms'. Retrieved 20 July 2011 from <http://www.slideshare.net/USArmySocialMedia/social-media-rounduppersonal-conduct-on-social-media-platforms>

US Army 2011c, 'US Army Brand Portal'. Retrieved 20 July from <https://www.us-armybrandportal.com/>

US Army 2011d, The United States Army social media handbook. Retrieved 20 July 2011 from <http://www.slideshare.net/USArmySocialMedia/army-social-media-handbook-2011>

US Army 2011e, 'Women in the U.S. Army'. Retrieved 20 July 2011 from <http://www.army.mil/women/>

US Navy 2010a, 'USS Abraham Lincoln Deploys video blogs'. Retrieved 20 July 2011 from <http://www.slideshare.net/USNavySocialMedia/ddocuments-and-setti>

US Navy 2010b, 'Apply FTC endorsement guides to social media best practices', Retrieved 20 July 2011 from <http://www.slideshare.net/USNavySocialMedia/applying-ftc-gguides-to-social-media-best-practices-snapshot>

Section 3.3.2 – Marketing – ADF practices and attitudes

DI(G) ADMIN 08-1 Public comment and dissemination of official information by Defence Personnel (available on Defence intranet only).

Snurb 2008, 'What if you build it and they do come?', gatewatching, 19 December 2008. Retrieved 14 July 2011 from <http://gatewatching.org/2008/12/19/government-consultation-online-what-if-you-build-it-and-they-do-come/>

Section 4.2 – Policy strategy framework

DI(G) ADMIN 08-1 Public comment and dissemination of official information by Defence personnel (available on Defence intranet only).

[viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFPbnxpZGNzeW5jfGd4OjYxYjZiYmY4ODZkYmQyNzg](http://www.slideshare.net/USNavySocialMedia/ddocuments-and-setti)

Dorsett J 2009b, 'Memorandum for the Information Dominance Corps – 2 November 2009'. Retrieved 25 July 2011 from <http://docs.google.com/>

