Research Article

Managing the risks of public discourse on the New South Wales Police Force *Facebook* Site

Andrew Kelly[†]

As of June 2013, the New South Wales Police Force had established 117 *Facebook* sites as part of its Project Eyewatch community-policing strategy. The strategy seeks to engage the public on the web in a way that allows people to lead their busy lives and still contribute to community-policing objectives. Internationally, few policing organisations have been as keen to embrace web communication with many officers skeptical about the value of web communication and others concerned about the risk of offensive, illegal or libelous comments being posted on police-managed websites. This study evaluates these risks in the context of the New South Wales Police Force's corporate *Facebook* site and considers the role of legislation, technology and self-regulation in managing risk. *Facebook* dialogue is examined for evidence of illegal, offensive, or objectionable content and the steps taken by the New South Wales Police Force to mitigate the risk are also considered. The study concludes that the risks of engaging the public on *Facebook* can be minimised and are far outweighed by the benefits, which include enhanced contact and engagement with the public.

Keywords: online policing, police communication, police *Facebook*, police social networking, Project Eyewatch, risk communication

INTRODUCTION

Police organisations internationally have recognised the need to engage with the public both in the real world where events happen and in the online world where many people choose to engage socially. Balancing the benefits of online community engagement with the risks is an ongoing concern for policing organisations. An errant or offensive comment made by a police officer or citizen at a public meeting is generally only shared with a small audience and is

[†] Corresponding author: akelly@csu.edu.au

easily addressed, whereas a similar remark typed on a police organisation's website can be shared worldwide and indelibly tarnish the reputation of that organisation and police more generally.

Most policing organisations have been slow to embrace web communication because of concerns about reputation, resourcing and liability arising from comments published on police websites that are discriminatory, unlawful, defamatory, private, in breach of copyright or otherwise objectionable. In recent years, many policing organisations have experimented with the use of social networking services such as *Twitter*, *Flickr*, and *YouTube*, but very few have embraced it to the extent of the New South Wales Police Force (NSWPF). The organisation began with one corporate *Facebook* site in 2008, but now has more than 117 *Facebook* sites as part of its Project Eyewatch strategy. Project Eyewatch evolved from the seminal community policing strategy Neighbourhood Watch and shares many of its community-based policing objectives.

This article is based on a study of the use of *Facebook* by the NSW Police Force, in which dialogue posted to the organisation's corporate *Facebook* site was analysed for evidence of objectionable content. It considers the role technology, legislation and self-regulation has in mitigating risk, as well as the specific steps being taken by the NSW Police Force to moderate its *Facebook* sites and to mitigate risk. The discussion is informed by a content analysis of 20 police postings, ten public postings and 347 public comments made on the NSW Police Force *Facebook* site on 31 August, 2011.

BACKGROUND

Internationally, governments are increasingly emphasising the need for public bodies to be more accountable, responsive and encourage citizen participation in priority setting and running local services (Jackson, & Bradford, 2010; Brainard & McNutt, 2010). However, the ability of police to share information with the public is restricted by judicial and investigative priorities. Police are in the difficult position of being criticised by the judiciary when they release too much information and by the media when they withhold information.

Most police organisations have a website but relatively few are using social networking services to their full potential; partly because of concerns about resourcing, reputation and liability and partly because of a lack of awareness of the potential for web technology to enhance policing (Vrielink,

2011; Cohen, 2010; Stevens, 2010). There is however a growing consensus among police managers that web technology has the potential to enhance police legitimacy and further community policing objectives (Crump, 2011; Rosenbaum, Graziano, Stephens & Schuck, 2011).

There are important differences between the online and real worlds in respect of legislation, civil rights and social norms (Wall, 2007; Williams, 2007; Blumstein, 2003; Greenleaf, 1998). The real world is defined by borders on a map, state sovereignty and homogenous cultures. These distinctions are less clear on the Internet, where the laws and regulations of one country can often be circumvented through the use of technology and nebulous jurisdiction.

The global connectivity of computer networks, the ability to instantly transmit large quantities of data and the Internet's lack of respect for national borders reinforce the differences with the real world (Chitsa, 2011). There is also a general resistance among Internet users to the regulation of cyberspace by any particular sovereign and a growing body of Internet users who are claiming independence from the physical world, rejecting terrestrial laws in preference to the emergent laws of the Internet (Williams, 2007).

Governments have had some success in regulating the Internet by enforcing laws that restrict access to certain content, by imposing regulations on Internet Service Providers and through bilateral agreements with international partners. For example, Article 10 of *The European Convention on Cybercrime* sought cooperation among member states to make it a criminal offence, in Europe at least, to infringe copyright on the Internet (Keyser, 2003).

Police organisations have varying approaches to social networking, with many embracing it as a strategic or operational imperative, some reluctantly entering into it because of the need to take control of sites widely believed to already belong to the police and others having limited or no web presence at all (McGovern, 2011). The use of social networking services by police in the United Kingdom has increased significantly since 2008 following an endorsement by the Association of Chief Police Officers (Crump, 2011).

In Australia, the Queensland Police Service, Victoria Police and the NSW Police Force are using *Facebook* for recruitment, public relations and operational purposes, while most Australian police organisations are also using *Twitter*, YouTube and *Flickr*. In Canada, police successfully used social networking to engage with the public and protesters during the 2010 G20 Conference in

Toronto (Stevens, 2010). Globally, there has been rapid growth in the use of web communication in all facets of policing.

Facebook is a web-based community that allows users to create profiles, share personal information and interests, post videos and photographs, and interact online with other members (Henson, Reyns & Fisher, 2011). According to *Facebook* (2013), there were 1.1 billion people who used their platform in March 2013, including more than 10 million users in Australia. There were also 751 million active users of *Facebook* on mobile devices. Aside from its potential to enhance engagement with the public, social media is a potential source of intelligence for police, a source of real-time information about policing issues, such as road accidents or emergencies, useful for those in the police who are directly engaged in protecting the public from harm on the Internet and as a tool for sharing knowledge with other policing organisations (Crump, 2011).

Formed in 1862, the NSW Police Force is one of the largest police organisations in the world, with more than 17,000 employees serving a population of seven million across an area of 801,600 square kilometres, comparable in size to United States state of Texas and double the combined geographic areas of England, Scotland, and Wales in Great Britain (NSW Police Force, 2012a). In August 2011 the NSW Police Force launched what could be seen as an ambitious community policing strategy centered on the establishment of *Facebook* sites at each of the state's 80 geographically-based local area police commands and many of its specialist squads. The decision by the NSW Police Force to drastically expand the organisation's social networking presence was made after a successful 18-month trial of its corporate *Facebook* site. While the NSW Police Force corporate *Facebook* site is administered centrally by the organisation's Police Media Unit, Project Eyewatch *Facebook* sites are de-centrally administered by local police.

The *NSW Police Force Media Policy* (2013) provides a framework for how the organisation controls the release of information, including its use of social networking services. The policy warns employees of the risks of defamation, privacy, contempt of court and interfering with investigations, and provides guidance about the circumstances police can release information. The policy is part of a risk mitigation strategy, which includes filtering technology and 24-hour monitoring by the NSW Police Force Media Unit (PMU) in order to protect against objectionable public discourse on the organisation's website.

At a local level, selected police officers are nominated to engage the public online and help moderate the *Facebook* dialogue. The public can post comments on the police *Facebook* sites but are now, subsequent to the data being obtained in this study, restricted from publishing videos, photographs and other links to project Eyewatch sites. The restriction was put in place after the organisation's *Facebook* site was maliciously targeted in 2011 by fans of a high-profile bodybuilder who was arrested by police.

WHAT ARE THE RISKS OF SOCIAL NETWORKING?

Complex jurisdictional, legislative and social issues make it difficult to assess the risk of public discourse on an organisation's social networking site and as a consequence public sector managers are often risk-adverse when it comes to engaging online in dialogic communication with the public (Shirky, 2008; Pickin *et al*, 2002). Police have three main concerns about the use of social networking services. First, they fear that employees will cause damage to the organisation's reputation by posting inappropriate content. Second, they fear being held accountable for objectionable comments made by members of the public on the organisation's website. Third, police acknowledge that the benefits of social networking outweigh the risks but often lack the resources to adequately manage those risks (Stevens, 2010).

The first concern is being addressed through internal policies that outline the behaviour expected of police officers when engaging online. The NSW Police Force (2012c) uses the real-life example of a male police officer who was a prosecution witness in an assault trial where, in order to discredit him as a witness, the defence lawyer tabled a *Facebook* picture of the officer appearing intoxicated and wearing a bikini. In the United Kingdom, initial concerns among the Association of Chief Police Officers about the impact of social networking on freedom of information procedures, court proceedings, information management and police communication have gradually been overcome with the development and release of new policies by local forces and by the National Policing Improvement Agency. The policy framework has led to a consensus among senior police that social media has a important part to play in engagement with the public and more resources are being directed towards this endeavour (Crump, 2011; NPIA, 2010).

Applying the laws of defamation, privacy, and copyright to policing and web communication is complicated by the varying circumstances that can arise

and the differences that exist between jurisdictions. In Australia, a person who carelessly or recklessly republishes or circulates a defamatory statement may be just as liable as the original author, even when the statement originated overseas (Blumstein, 2003; Vick, McPherson & Cooper, 1999). For example, an Australian plaintiff sued the publishers of *The Wall Street Journal* in Victoria for statements it had published online that implied he was a money launderer. While the publisher is partially protected in the United States by the constitutional First Amendment right of free speech, the Australian High Court held that action could be taken against the publisher in any place where the comments are published (Chitsa, 2011). The level of editorial control a publisher has over the content is also an important consideration of liability in defamation matters. The more control the more liable the publisher is if they have failed to exercise that control responsibly (Decarlo, 1997).

Ibrahim (2008) characterised online networks as ‘‘complicit risk communities where personal information becomes social capital which is traded and exchanged’’ (p. 251). Users of social networking sites are often prepared to give up some privacy because of the social capital gained from being part of an online network (Debatin, Lovejoy, Horn & Hughes, 2009). Privacy is often breached when third parties target the data of social networking services for personal information and for other malicious purposes such as hacking and identity theft (Boyd and Ellison, 2008). Organisations have a social and legal responsibility to protect the personal information of their subscribers. For example, Vodaphone Australia was referred to the Australian Office of the Privacy Commissioner after the billing and call records of four million customers were mistakenly posted onto a public website (Martin & Battersby, 2011).

One of the key objectives of community policing is to inform the public about local crime and policing issues although such discussions are fraught with risk to the judicial process (Kingshott, 2011). The *NSW Police Force Media Policy* warns of the need for police to balance the public’s right for information against the integrity of the investigative and judicial processes (NSW Police Force, 2013). Police can limit the information provided in a media release but are less able to restrict contemptuous comments posted by the public to the organisation’s websites.

Since the 1970s, police have generally restricted the release of information to the public, often drawing criticism from the media for a lack of transparency and giving rise to speculation about police investigations (Egan, 2011).

Managers must continually balance the risks of social networking and the expected benefits of creating and maintaining interpersonal relationships (Debatin *et al*, 2009; Ibrahim, 2008; Tufekci, 2008; Tyma, 2007).

THE BENEFITS OF SOCIAL NETWORKING

The use of new media technologies has enabled police to communicate with the public more efficiently and cost effectively, while also enhancing the professional status and legitimacy of police organisations and their claims of transparency and public accountability (McGovern, 2010; Chan, Goggins & Bruce, 2010). Technology has fundamentally changed the way police organisations interact with the media and also in the way the media reports crime and policing news. Cuts to newsroom expenditure, a decline in the number of crime reporters and the unrelenting demands of a 24-news cycle have left media organisations with little choice, but to rely on the information provided by police media units (Mawby, 2010; McGovern, 2010; McGovern & Lee, 2010).

Many police organisations are choosing to bypass the media altogether when engaging the public to avoid the potential for the media to impose their own biases and frames on the intended message (Economou, 2009). Public attitudes to news are also changing as the Internet becomes an increasingly important source of information. In just three days during a flood crisis in January 2011, more than 150,000 people joined the Queensland Police Service *Facebook* site in order to receive emergency services updates. Conversely, Queensland's biggest selling newspaper, the *Courier Mail*, only increased its online membership by a few thousand during the crisis (Traffika, 2011).

> This isn't to say that the *Courier Mail* did a worse job than the Queensland Police Service, as the newspaper had a lot more stories to cover across a broader range of topics. What it does show, however, is the effect of providing relevant, on-topic content to a market in need, versus more general content to a broader market. (Traffika, 2011)

The emergence of the Internet has led to a renewed examination of how police organisations interact with the public. For police, community engagement once meant meetings at the town hall, coffee shops, local churches or public squares but the Internet has generated a new public sphere, one where there has been a fundamental change to community and communication (Holmes, 2005). Enhancing the visibility of police, improving the quantity and quality of personal contact, and providing the public with information about local crime and

policing issues have all been shown to enhance the public's confidence in the police (Bradford, Stanko & Jackson, 2009). As the number and size of online communities has increased, so too has the need for police to establish a visible online presence to engage with these communities.

REDUCING THE RISK OF SOCIAL NETWORKING

There are three forms of control that can help reduce the risks of social networking: legislative; technological; and human. Legislative control is complicated by jurisdictional issues and the pervasive idea that cyberspace is free and distinguishable from the real world (Williams, 2007). The *European Convention on Cybercrime* is an example of legislative controls being used to reduce the risks of communication on the Internet. In Australia, the Federal Government has been considering introducing mandatory filters for Internet communication since 2007, primarily to protect children from harmful content (Duffy, 2009).

The use of technology is regarded by many as a more effective way to regulate cyberspace (Wall, 2007; Williams, 2007; Lessig, 1999). Technology can disrupt human action; impose constraints on how content is accessed and distributed; can be instituted pervasively and with immediacy; is adaptive to changes in law, societal norms, market influences or cyber threats; is less contentious than regulation; and is preventative rather than punitive (Williams, 2007, p. 77). Social networking services also have embedded technological solutions for protecting organisations against risk. For example, the NSW Police Force uses the *Facebook* blocking tool to filter objectionable words, including "bastard", "mongrel", and "chestbrah" (a reference to the bodybuilders). The word "court" is blocked, too, to minimise the risk of contemptuous commentary on judicial proceedings.

Employees assigned to moderate an organisation's website play an important role in educating users and reinforcing an organisation's social networking policy (Herring, Job-Sluder, Scheckler & Barab, 2002). Moderator engagement with the site's membership can also help ensure important corporate messages are not ignored or missed (Regester & Larkin, 2008). Studies have shown that online forums generally comprise a homogenous membership of active and passive supporters who will do what they can to maintain the norms of the group, reducing the need for moderator vigilance (Farsangi, 2010; Bruggeman, 2008; Boyd & Heer, 2006; Dahlberg, 2001). *Wikipedia* operates on

this premise, promoting user-generated quality control not as a legal obligation but as a commitment to its educational purpose and to the diligence of its fact-checking community (Walsh & Oh, 2010).

RESEARCH DESIGN AND DATA

The NSW Police Force employs a fulltime digital media assistant to monitor its social networking sites and remove objectionable comments. While the majority of public comments on the NSW Police *Facebook* site can be openly accessed by any *Facebook* user at any time, it is only possible to capture the deleted and filtered comments at the time of their removal. As such, it was necessary for the researcher to be present with the digital media assistant as the comments were removed. Permission was only granted for the researcher to attend the Police Media Unit for one day, limiting the amount of data obtained. As such, the findings of this study are limited to a one day sample and, while useful for informing the discussion at hand, the findings are indicative rather than definitive.

Only public comments made on the site up to midday on the day following the initial posting were able to be considered, allowing the public between 13 and 32 hours to post a comment on the relevant entries. A check of the entries a week later revealed that only a small number of additional comments had been added, indicating that most responses occurred in the hours following the initial posting.

Facebook Insights data for the month of August 2011 was provided by the NSW Police Force. Wednesday, 31 August 2011 was an average day for the NSW Police Force *Facebook* site. Police posted 20 items on the *Facebook* wall, generating 317 public comments and attracting between 5,000 and 50,000 impressions for each item (impressions are the number of times a post is viewed anywhere on *Facebook*). See table 1.

Item 16 was removed from the site by the digital media assistant's manager on 1 September, 2011 after a number of objectionable comments were posted and because of an expectation that the item would continue to attract objectionable comments. The manager and other Police Media Unit staff have administrative access to the corporate *Facebook* site and are able to delete and post comments, videos, pictures and links. Members of the public posted a further 10 items that were unrelated to the police postings, eliciting 30 comments

from other users. None of these items or the comments they elicited were removed by the site's moderators. See table 2.

Upon logging into the NSW Police Force *Facebook* site on 1 September 2011, the digital media assistant identified 17 public comments from the previous day that had been filtered by the *Facebook* blocking tool. A review of the postings was conducted and 11 items were left unpublished and six were permitted to be published. A further eight comments, which were not identified by the site's filter, were deleted by the moderator. About 5.5 per cent of the comments made on the NSW Police Force *Facebook* site on 31 August, 2011 were not published. See table 3.

The following are examples of the comments that were filtered:

- "Sicko bastard"
- "I hope you get the mongrel"
- "Shame on the NSW court system"
- "Police do their jobs but the court system lets them down"
- "Damned if they do, rip their friggen head off"
- "Justice system fucked, shit, cunt..."

A number of mentions of the word "court" were at first filtered but later published by the moderator because the context of the comment was not considered to be contemptuous. Comments that cleared the filter but were later deleted by the moderator included:

- "Bring back the death penalty"
- "I recommend surgical removal of the body part that touches the child"
- "Castration comes to mind"
- "He should have been shot on the spot"
- "No point wasting the court's time"
- "I blame the owners for neglect and believe the boy provoked the dog attack"
- "Psycho"

Derivatives of blocked words such as court, for example "courts", were able to clear the filter, while there were also occasions when colloquial, expletive and profane words were published despite there being some likelihood that these

words might be deemed as offensive in some real-world contexts. Examples of potentially objectionable comments that cleared both the filter and the moderator included:

- "Another moron off the streets"
- "Great more dick heads running around with guns and in my own backyard too"
- "Them idiots"
- "I remember Green Valley when I was a kid. Same with all the western suburbs. Now murder, rape, bashing, drugs... filth in general"
- "The ONLY good (outlaw) bikie is a DEAD one!!! As long as they are not harming the general public, leave them to it!"
- "People should be put down not dogs"
- "Youth conference! Pathetic! Serial killer in the making! Anyone who harms defenceless animals and small children should be locked away"

RESEARCH FINDINGS

Facebook Insights reveals that as of 31 August, 2011, the NSW Police Force *Facebook* site had attracted 57,260 likes (subscribers), with 4,085 of those people later unsubscribing. About 62 per cent of users accessing the site are female, 35 per cent are male and three per cent are not specified. About 92 per cent of users are identified as being from Australia and 74 per cent are identified as being from NSW. During August 2011, there were 9,904 comments made on the site, averaging 320 a day, the lowest being 189 on Sunday, 7 August and the highest 515 on Wednesday, 17 August. There were 552,255 unique visitors to the site during August 2011, with an average of 17,815 people accessing the NSW Police *Facebook* site each day.

Of all the items posted on 31 August, Item 16 (Police confirm child's death as suspicious) was the most provocative. The item was posted by police at 6.02pm on 31 August and removed the next morning about 10am. During this period of publication, 79 comments were posted by the public to the NSW Police Force *Facebook* site. Six of these items were blocked by the site's filter and one item was deleted by the moderator the next morning before the entire posting was removed. The dialogue that took place on the site overnight included one entry that purported to name the child, several entries that discussed the specific location of the incident and the family's involvement with authorities, some that

linked media reports to the information provided by the police and many others that opined on the values and conduct of the family concerned. The forum discussion initiated by the police led, in a very short time, to the publishing of information that could identify the dead child and her family, which is illegal under NSW law. It included a number of comments that arguably impugned members of the child's family and breached their privacy by revealing their street address and involvement with government agencies such as the NSW Department of Community Services.

Of the remaining postings, Item 4 (Boy injured in dog attack), Item 9 (Police investigate serious collision) and Item 19 (Police investigate child abduction) attracted the most comments from the public. The common factor in each of these incidents was the involvement of a child, including a nine-year-old girl (Item 19), a 13-year-old boy (Item 9) and an 11-year-old boy (Item 4). Six comments were filtered or deleted in Item 19 and one in Item 4, demonstrating a propensity, albeit from a very small sample, for postings about harm to children to elicit objectionable comments on the *Facebook* forum. Of the items initiated by the public, a discussion on the use of fog lights by motorists attracted the most interest with 22 comments.

There were numerous comments by users attempting to control the dialogue on the forum, admonishing extreme comments and steering the conversation to the information provided in the police media release. There was nil evidence of the site moderator being influenced by user comments. For instance, none of the decisions made by the moderator to change, add or delete content were made on the basis of a user request or comment. The literature suggests that the behaviour of online users is influenced by their online peers (Boyd & Heer, 2006); however this study does not provide any data to support or refute this claim.

DISCUSSION

The first objective of this study was to provide police practitioners and scholars with a better understanding of the risks that can arise when engaging the public on *Facebook*. The data obtained from the NSW Police *Facebook* site on 31 August, 2011 contained clear examples of offensive, unlawful, contemptuous and defamatory comments, with more than five per cent of comments considered by the NSW Police Force to be unpublishable because of their objectionable content. The evidence from the literature is that when such comments are posted

on an organisation's website, the organisation is often as liable as the person who posted the comment. Disparately, the literature also suggests that *Facebook* and other social networking services can benefit the police by helping them to communicate with the public more efficiently and cost effectively, while also enhancing the professional status and legitimacy of police organisations and their claims of transparency and public accountability.

Although the sample used in this study was too small to make definitive findings, it was useful for demonstrating the effectiveness of technology and human moderation in managing the risks, with most of the objectionable comments posted by the public either filtered or deleted within one day of being posted. The presence of sufficient and knowledgeable staff to moderate the organisation's social networking services ensured that objectionable comments were quickly removed and that legitimate public comments filtered by *Facebook*'s blocking tool were reinstated. The moderator's knowledge, experience and awareness of legislation, organisational policy and policing would appear to be an important factor in reducing the risks of engaging the public online.

It was evident from the research that the process of monitoring and moderating the organisation's *Facebook* site can also help police to understand their organisational and operational environment, helping to inform operational practices and to develop policies and mechanisms by which they operate (Herrington, 2011; Stanko, 2010). For example, the site's administrators would now be aware that posting information relating to children is likely to elicit a significant response from the public and that there exists a greater risk of objectionable comments being posted. The organisation can reduce the risks by not posting inflammatory media releases to the *Facebook* site, by increasing the lexicon of objectionable words in the filter and by being vigilant moderators of the site.

The death of a child is a matter of significant public interest and it is common for police to release information about their investigation to the media, as occurred with Item 16 (Police confirm child's death as suspicious). In this instance it was probably necessary, in accordance with organisational policy, for police to release information in order to "provide transparency and maintain community faith in policing and our system of justice" (NSW Police Force, 2013, p. 4). However, the release of information through a media release poses less risk to the organisation than hosting of a public online forum to discuss the information

contained in the release. The removal of the item by the Police Media Unit appears to be recognition of the risks that presented on *Facebook* and for the organisation to be selective about the topics it chooses to engage the public in two-way communication.

The small percentage of deleted and filtered comments should not be viewed as confirming that the remaining comments were free of unlawful, liable or offensive content. Rather, it indicates that the site's moderators, based on their understanding of the relevant legislation, regulations, policies and organisational standards, did not regard the majority of comments as a risk to the organisation. The removal of Item 16 from the *Facebook* site reflects how police can quickly and easily remove threads that prompt objectionable comments provided adequate resources have been allocated to monitor the organisation's social networking sites. Additionally, when the organisation's *Facebook* site is deluged by objectionable comments, as occurred with the bodybuilder incident, words such as "chestbrah" can be added or removed from the filter, reducing the burden of the moderator through the use of technology. The willingness of Internet users to self-moderate their comments can also limit the risks of online forum communication.

Each of the items posted by police on the *Facebook* site was linked to a media release issued simultaneously by the organisation to the mainstream media. *Facebook* Insights shows that each item was viewed between 5000 and 50,000 times within one day of being posted to the Internet. As membership of the NSW Police Force *Facebook* site increases, so too does the organisation's potential audience and the associated benefits of engaging with that audience. This study does not compare the *Facebook* and mainstream media audience numbers but it does highlight that there are real and emerging communities that the police can communicate directly with in an efficient, cost effective and transparent manner.

CONCLUSION

Future studies would benefit from a larger sample of data that includes case studies from other policing organisations and a longer observation period. While the quantity of data obtained in this study was limited, it did serve the purpose of highlighting the issues faced by modern police organisations in relation to the risks and benefits of using social media services such as *Facebook*.

The NSW Police Force is an example of a policing organisation that has been willing to accept the risks of engaging with the public online although it has done so with the appropriate risk mitigation measures in place. The study showed that more than five per cent of public comments posted to the NSW Police Force *Facebook* site were objectionable, meaning they had the potential to harm the reputation of the organisation or expose it to litigation. However, the use of technology and human moderation considerably reduced the risks, eliminating many but not all of the objectionable public comments.

The remaining risk is offset by the considerable benefits that arise when police engage in two-way communication with the public, including enhanced public confidence and trust in the police.

REFERENCES

Archbold, C.A. (2005). Managing the bottom line: risk management in policing, Policing: An International Journal of Police Strategies & Management, Vol. 28 (1), 30-48.

Bennett, T., Holloway, K. & Farrington, D.P. (2009). A review of the effectiveness of Neighbourhood Watch, *Security Journal* (22), 143-155.

Blumstein, S. (2003). The new immunity in cyberspace: The expanded reach of the Communications Decency Act to the libellous "re-poster", *Boston University Journal of Science and Technology Law*, Vol. 9 (2).

Boyd, D., & Ellison, N. B. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13, 210–230.

Boyd, D. & Heer, J. (2006). Profiles as Conversation: Networked Identity Performance on Friendster. *Hawaii International Conference on System Sciences*, Vol. 3, 59c, Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) Track 3, 2006.

Bradford, B., Stanko, E.A. & Jackson, J. (2009). Using research to inform policy: The role of public attitude surveys in understanding public confidence and police contact. *Policing*, Vol. 3 (2), 139-148.

Brainard, L.A. & McNutt, J.G. (2010). Virtual government – citizen relations: Informational, transactional or collaborative. *Administration & Society*, 2010 (42), 836-858.

Bruggeman, J. (2008). *Social networks: An introduction.* Routledge Publishers, London and New York.

Chan, J., Goggins, G. & Bruce, J. (2010). 'Internet Technologies and Criminal Justice', in Y. Jewkes & M. Yar (Eds) *Handbook of Internet Crime*, Willan Publishing, Devon, 582-602.

Chitsa, S. (2011). Name Calling On The Internet: The Problems Faced By Victims Of Defamatory Content In Cyberspace, *Cornell Law School Inter-University Graduate Student Conference Papers.* Paper 48. http://scholarship.law.cornell.edu/lps_clacp/48.

Cohen, L.S. (2010). *6 Ways Law Enforcement Uses Social Media to Fight Crime.* Retrieved on 12 November, 2011 from: http://mashable.com/2010/03/17/law-enforcement-social-media/.

Crump, J. 2011. What are the police doing on Twitter? Social media, the police and the public. *Policy & Internet* Vol. 3, (4), Article 7, 1-27.

Dahlberg, L. (2001). Computer-mediated communication and the public: A critical analysis. *Journal of Computer-Mediated Communication, Vol. 7 (1*), cited in Kushin, M.J. & Kitchener, K. (2009). Getting political on social network sites: Exploring online political discourse on Facebook. *First Monday, Vol. 14 (11).*

Debatin, B., Lovejoy, J.P., Horn, A.K. & Hughes, B.N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences Journal of Computer-Mediated Communication 15 (2009) 83–108.

DeCarlo, K.J. (1997). Tilting at windmills: Defamation and the private person in cyberspace, Georgia State University Law Review Vol. 13, 547- 579.

Duffy, J.M. (2009). Toothless tiger, sleeping dragon: Implied freedoms, filters and the growing culture of censorship in Australia. eLaw Journal: Murdoch University Electronic Journal of Law, Vol 16 (2).

Economou, M. (2009). *Law Enforcement Working as Journalists.* Retrieved on 14 January, 2011 from http://connectedcops.net/?p=916.

Egan, A.B. (2011). The NYPD: The nation's largest police department as a study in public information, *Public Relations Journal* Vol. 5 (2) Spring 2011.

Facebook (2013). Facebook statistics. Retrieved on 6 June, 2013 from http://newsroom.fb.com/Key-Facts

Farsangi, M.H. (2010). *Active citizens on Facebook: Case study of Indonesians' online participation regarding the 2009 presidential election*. Australian New Zealand Communication Association 2010 Conference, Canberra,

retrieved on 20 April, 2011 from http://www.anzca.net/conferences/conference-papers/94-anzca10proceedings.html.

Greenleaf, G. (1998), An endnote on regulating cyberspace: Architecture versus law?'', *University of New South Wales Law Journal*, Vol. 21, 593-622.

Hearn, L. (2011). Flock to Facebook for flood updates. *Sydney Morning Herald*, 11 January, 2011. Retrieved on 14 May, 2012 from http://www.smh.com.au/technology/technology-news/flock-to-facebook-for-flood-updates-20110111-19mfr.html.

Henson, B., Reyns, B,W. & Fisher, B.S. (2011). Security in the 21st Century: Examining the link between online social network activity, privacy, and interpersonal victimization, *Criminal Justice Review* 36, 253.

Herring, S., Job-Sluder, K., Scheckler, R. & Barab, S. (2002). Searching for safety online: Managing trolling in a feminist forum. *The Information Society,* 18: 371-384.

Herrington, V. (2011). Police as critical consumers of research: informing practice through research, in Birch, P. & Herrington, V. (Eds). *Policing in practice*, Palgrave McMillan, South Yarra, Australia.

Holmes, D. (2005). *Communication theory: Media, technology and society.* Sage Publications, London.

Ibrahim, Y. (2008). The new risk communities: Social networking sites and risk. *International Journal of Media & Cultural Politics*, 4(2), 245–253.

Jackson, J. & Bradford, B. (2010). What is trust and confidence in the police*? Policing*, Vol. 4 (3), 241-248.

Johnson, D. R. & Post, D. (1996), ''Law and borders: The rise of law in Cyberspace'', *Stanford Law Review*, Vol. 48, 1367-1380.

Keyser, M. (2003). The Council of Europe Convention of Cybercrime, *Journal of Transnational Law and Policy*, Vol. 12 (2), 287-326.

Kingshott, B.F. (2011): Effective police management of the media, *Criminal Justice Studies*, 24 (3), 241-253.

Lessig, L. (1999), *Code: And Other Laws of Cyberspace*, Basic Books, New York.

Martin, P. & Battersby, L. (2011). Vodafone may be liable on privacy breach. *Sydney Morning Herald*, January 10, 2011.

Mawby, R. C. (2010) 'Police Corporate Communications, Crime Reporting and the Shaping of Crime News', *Policing and Society*, vol 20 no 1, 124-39.

McGovern, A. (2010). *Tweeting the News: Criminal Justice Agencies and their Use of Social Networking Sites*. The Australian and New Zealand Critical Criminology Conference 2010 (c) 2011 Institute of Criminology, Sydney Law School, The University of Sydney http://sydney.edu.au/law/criminology.

McGovern, A. (2011). Tweeting the News: Criminal justice agencies and their use of social networking sites, *The Australian and New Zealand Critical Criminology Conference Proceedings 2010*, Sydney Institute of Criminology, retrieved on 10 May, 2012 from http://hdl.handle.net/2123/7378

McGovern, A. & Lee, M. (2010). Cop[ying] it sweet: Police media units and the making of news, The Australian and New Zealand Journal of Criminology, Vol. 43 (3), 444-464.

NPIA. 2010. *Engage: Digital and Social Media for the Police Service.* London: National Policing Improvement Agency.

NSW Police Force (2012a). *NSW Police Force*, retrieved on May 22, 2012 from http://www.police.nsw.gov.au

NSW Police Force (2013). *NSW Police Force Media Policy, retrieved on 17 June, 2013 from* http://www.police.nsw.gov.au/__data/assets/pdf_file/0003/175269/Media_Policy_4_February_2013_FINAL.pdf

NSW Police Force (2012c*). Personal Use of Social Media Policy and Guidelines*. (August 2011), Retrieved on 13 November, 2011 from http://www.police.nsw.gov.au/__data/assets/pdf_file/0007/208609/personal-use-of-social-media-policy-and-guidelines.pdf.

NSW Police Force (2012d). *New South Wales Police Facebook site*, Retrieved 22 May, 2012 from https://www.facebook.com/nswpoliceforce.

Pickin, C., Popay, J., Staley, K., Bruce, N., Jones, C. & Gowman, N. (2002). Developing a model to enhance the capacity of statutory organisations to

engage with lay communities, *Journal of Health Services Research & Policy*, Vol. 7 (1), 34-42.

Queensland Police Service (2011). *Queensland Police Service Facebook page*. Retrieved on 21 November, 2011 from https://www.facebook.com/QueenslandPolice.

Reiner, R. (2000). *The Politics of the Police (3rd Ed.)* Oxford University Press, Chapter 5: Mystifying the police: The media presentation of policing. 138-163.

Regester, M. & Larkin, J. (2008). 4th Ed. *Risk issues and crisis management in public relations: A casebook of best practice*. Kogan Page, London.

Rosenbaum, D.P., Graziano, L.M., Stephens, C.D. & Schuck, A.M. (2011). Understanding community policing and legitimacy-seeking behaviour in virtual reality: A national study of municipal police websites. *Police Quarterly*, 2011 (14), 25-47.

Shirky, C. (2008). *Here comes everybody. The power of organising without organisations*, Penguin Books, New York.

Socialbakers (2012). *Australia Facebook statistics*. Retrieved on 2 May, 2012 from http://www.socialbakers.com/facebook-statistics/australia

Stanko, E.A. (2010). Improving policing through research. *Policing: A Journal of Policy and Practice*, Vol. 3 (4) 306-309.

Stevens, L. (2010). When cops are attacked with social media: eight lessons *learned at G20*. Retrieved on 5 January, 2011 from http://connectedcops.net/?p=2230.

Tankard, J.W. (2001). The empirical approach to the study of framing. In S.D. Reese, O.H. Gandy Jr. and A.E. Grant (Eds.), *Framing public life*, Lawrence Erlbaum Associates, Mahwah, NJ, 95-106.

Traffika (2011). *Queensland Police Helps Us Stay Above Water*. Retrieved on 14 May, 2012 from http://www.traffika.com.au/blog/article/queensland-police-helps-us-stay-above-water

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1), 20–36.

Tyma, A. (2007). Rules of Interchange: Privacy in online social communities: A rhetorical critique of MySpace.com. *Journal of the Communication, Speech & Theatre Association of North Dakota*, 20, 31–39.

Vick, D.W., Macpherson, L. & Cooper, S. (1999). Universities, Defamation and the Internet *The Modern Law Review Limited* 1999 62:1, January). Blackwell Publishers, Oxford, USA.

Vrielink, R. (2011). The use of social media within police education. *School of Policing, Police Academy of the Netherlands.*

Wall, D. (2001). Maintaining order and law on the Internet, in D.Wall (Ed.),*Crime and the Internet*, Routledge, London.

Wall, D. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace, Police Practice and Research, Vol. 8. (2), 183-205.

Walsh, K.M. & Oh, S. (2010*). Self-Regulation: How Wikipedia Leverages User-Generated Quality Control Under Section 230*, Express, Available at http://works.bepress.com/sarah_oh/1.

Williams, M. (2007). Policing and Cybersociety: The Maturation of Regulation within an Online Community, *Policing and Society*, 17:1, 59-82.

ABOUT THE AUTHOR

Andrew Kelly, BA, MA, is a lecturer and early-career researcher with Charles Sturt University's School of Policing Studies, Goulburn, New South Wales. He worked as a police officer, journalist, and corporate communications manager with various government organisations before commencing his academic career. His current research focuses on the use of online social media by policing organisations to engage with the public.

TABLES

Table 1—Police *Facebook* postings 31 August 2011

	Title of posting	Time	Number of comments made by the public
1	Police investigate fire at unit block	3.43am	1
2	Man dies after being hit by runaway trailer	3.58am	21
3	Police appeal after lamb dies following cruel attack	4.27am	27
4	Boy injured in dog attack	4.56am	39
5	Police locate vehicles following investigations into shooting	9.02am	3
6	Firearms stolen from house during break and enter	9.03am	14
7	Police charge man following alleged sexual assault	9.07am	9
8	Man charged following armed robbery and assault	10.53am	3
9	Police investigate serious collision	11.00am	28
10	Police attend stabbing incident	12.16pm	6
11	Man arrested after drugs, firearm and ammunition located	12.48pm	12
12	Police officer recognised with courage award	2.47pm	6
13	Car crashes into house	5.04pm	7
14	World War II firearms stolen	5.10pm	8
15	Police appeal for information about stabbing	5.12pm	6

16	Police investigate child's death	6.02pm	79
17	Family stuck overnight in vehicle	6.15pm	10
18	Three arrested over shooting	9.23pm	5
19	Police investigate child abduction	10.19pm	31
20	Man injured during violent assault	11.12pm	2
		Total	317

Table 2: Civilian postings to *Facebook* 31 August 2011

	Nature of posting	Total comments
1	Enquiry – toddler run over	0
2	Enquiry – MVA	0
3	Enquiry – disturbance	4
4	Enquiry – disturbance	1
5	Enquiry –disturbance	0
6	Notification – Traffic backup M5	0
7	Complaint –fog lights	22
8	Enquiry – wish I could be a copper	1
9	Enquiry – disturbance	0
10	Enquiry – crime statistics	2
	Total comments	30

Table 3: Number deleted, filtered, and published comments

	Title of posting	Deleted	Filtered	Published	Total
1	Police investigate fire at unit block	0	0	1	1
2	Man dies after being hit by runaway trailer	0	0	21	21
3	Police appeal after lamb dies following cruel attack	1	0	26	27
4	Boy injured in dog attack	1	0	38	39
5	Police locate two vehicles following investigations into shooting	0	0	3	3
6	Firearms stolen from house during break and enter	0	1	13	14
7	Police charge man following alleged sexual assault	2	0	7	9
8	Man charged following armed robbery & assault	0	0	3	3
9	Police investigate serious collision	0	0	28	28
10	Police attend stabbing incident	0	0	6	6
11	Man arrested after drugs, firearm and ammunition located	0	0	12	12
12	Police officer recognised with courage award	0	0	6	6
13	Car crashes into house	0	0	7	7
14	WWII firearms stolen during break-in	0	0	8	8
15	Police appeal for information over stabbing	0	1	5	6

16	Police confirm child's death as suspicious	1	6	72	79
17	Family stuck overnight after vehicle caught in mud	0	0	10	10
18	Three arrested by Greenacre shooting investigators	0	0	5	5
19	Police investigate child abduction	3	3	25	31
20	Man injured during violent assault	0	0	2	2
21	Public wall posts	0	0	30	30
	Total	8	11	328	347

- o O o -