Social Media and Law Enforcement

Commissioner for Law Enforcement Data Security

July 2013
Social Media and Law Enforcement

Commissioner for
Law Enforcement Data Security

July 2013
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Executive Summary</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>Background</td>
<td>6</td>
</tr>
<tr>
<td>1.1</td>
<td>The Internet, the Web and Social Media</td>
<td>6</td>
</tr>
<tr>
<td>1.2</td>
<td>Social Media, Mass Communication and New Business Models</td>
<td>8</td>
</tr>
<tr>
<td>1.3</td>
<td>Examples of Social Media</td>
<td>9</td>
</tr>
<tr>
<td>1.4</td>
<td>Social Media’s ‘Ubiquity’</td>
<td>10</td>
</tr>
<tr>
<td>1.5</td>
<td>The Rise of Social Media in Law Enforcement</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>Victoria Police</td>
<td>14</td>
</tr>
<tr>
<td>2.1</td>
<td>Background</td>
<td>14</td>
</tr>
<tr>
<td>2.2</td>
<td>The Approach to the Use of Social Media by Victoria Police Members</td>
<td>15</td>
</tr>
<tr>
<td>2.2.1</td>
<td>Official Use of Social Media by Victoria Police Members</td>
<td>15</td>
</tr>
<tr>
<td>2.2.2</td>
<td>Personal Use of Social Media</td>
<td>16</td>
</tr>
<tr>
<td>2.3</td>
<td>Victoria Police and ‘Digital Natives’</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>Victoria Police &amp; Social Media</td>
<td>18</td>
</tr>
<tr>
<td>3.1</td>
<td>Community Engagement</td>
<td>18</td>
</tr>
<tr>
<td>3.1.1</td>
<td>Facebook</td>
<td>19</td>
</tr>
<tr>
<td>3.1.2</td>
<td>Eyewitness</td>
<td>19</td>
</tr>
<tr>
<td>3.1.3</td>
<td>Twitter</td>
<td>20</td>
</tr>
<tr>
<td>3.1.4</td>
<td>YouTube</td>
<td>20</td>
</tr>
<tr>
<td>3.1.5</td>
<td>Instagram</td>
<td>21</td>
</tr>
<tr>
<td>3.1.6</td>
<td>Blogspot</td>
<td>21</td>
</tr>
<tr>
<td>3.1.7</td>
<td>Wikipedia</td>
<td>21</td>
</tr>
<tr>
<td>3.2</td>
<td>Passive Intelligence and Criminal Investigation</td>
<td>22</td>
</tr>
<tr>
<td>3.3</td>
<td>E-Crime Squad</td>
<td>23</td>
</tr>
<tr>
<td>3.4</td>
<td>Active Intelligence and Covert Operations</td>
<td>23</td>
</tr>
<tr>
<td>3.5</td>
<td>Internal Intelligence</td>
<td>24</td>
</tr>
<tr>
<td>3.6</td>
<td>Recruitment</td>
<td>24</td>
</tr>
<tr>
<td>3.6.1</td>
<td>Twitter Recruit</td>
<td>25</td>
</tr>
<tr>
<td>3.7</td>
<td>Enforcement</td>
<td>26</td>
</tr>
<tr>
<td>3.8</td>
<td>Case Study: Piloting the Operational Use of Facebook</td>
<td>26</td>
</tr>
</tbody>
</table>
4 Issues, Benefits and Risks

4.1 Introduction

4.2 Social Media Benefits

4.2.1 Social Media as a Source of Intelligence
4.2.2 Emergency Management
4.2.3 Community Engagement
4.2.4 Reputation Management

4.3 General Legal & Regulatory Issues

4.3.1 Social Media Terms of Service
4.3.2 Jurisdiction
4.3.3 Social Media and Criminal Investigations
4.3.4 Social Media’s Impact on Other Laws

4.3.4.1 Intellectual Property
4.3.4.2 Privacy

4.4 Specific Regulatory Issues

4.4.1 Victorian Public Records and Social Media
4.4.2 CLEDS Act & Standards

4.5 Control

4.5.1 Data Security
4.5.2 Community Expectations
4.5.3 Unauthorised Disclosure
4.5.4 Reputation Management

4.6 Resourcing

4.6.1 Staffing
4.6.2 Training
4.6.3 Return on Investment

4.7 Governance and Policy

4.8 Final Comments
Executive Summary

We are used to living in a world in which the internet provides the foundation for communicating, gathering and disseminating information. We also realise that the World Wide Web (web) is subject to ongoing innovation and development. The emergence of web-based social media, however, has been viewed as ground breaking, if not representing a paradigm shift. Certainly, social media’s depth of penetration is such that it cannot be ignored. Likewise, its impact upon policing is viewed as pivotal:

… [any] failure by police to adequately understand and utilise social media will result in a disengaged and irrelevant force.¹

In late 2011, CLEDS could see that a distinct discourse about social media and its use for law enforcement purposes was emerging, both within Australia and around the world.² At a minimum, this was relevant to CLEDS’s role in overseeing Victoria Police’s adherence to information security standards. In light of social media’s profile and depth of penetration, it was considered likely that there were broader issues and risks involved in the use of social media for policing purposes than information security alone.

Brief early discussions with other Australian police jurisdictions (in particular, the New South Wales Police Force), highlighted the fact that all Australian jurisdictions were in a similar position: on the one hand, police were already using social media for discrete policing functions but, on the other, it was occurring in a relatively ad hoc manner and the use of social media was not integrated as a standard tool across all police operations. It was apparent that similar issues relating to governance, law and regulation, policy, resourcing and technology arose in every jurisdiction.

In July 2012, CLEDS commenced a review of Victoria Police’s use of social media. The aim of the review was to identify the benefits, risks and challenges that the use of social media poses to Victorian law enforcement data security and integrity and law enforcement data systems.

As part of the review, CLEDS conducted considerable desktop research on social media and law enforcement and commissioned an introductory paper from academic experts in the field.³ The findings from these review processes were used to inform a social media issues paper, which was drafted to facilitate discussion at a Social Media and Policing Roundtable convened by CLEDS in February 2013. The roundtable brought together a range of social media, academic and law enforcement experts who were asked to provide feedback on the issues paper, including confirming, removing and/or adding risks, issues and opportunities and making recommendations about social media and policing.

This report is based on that issues paper with amendments reflecting the outcomes of the roundtable. It seeks to describe social media in terms of its place in the development of the web. Taking the position that social media already has a place in the arsenal of policing tools and, further, that it is becoming increasingly important, the paper documents how social media is currently being used within law enforcement – principally in relation to Victoria Police. It also seeks to identify some of the more significant opportunities, issues and risks that social media presents in the execution of law enforcement functions. While some of these issues and risks are manageable, subject to appropriate risk management, others are not so easily resolved. This suggests that social media may not be capable of providing a complete or comprehensive platform for all law enforcement functions and activities, at least in the short term.

---

¹ Pearls in Policing, Summary report, 2011.
² See, for example, Professor Andrew Goldsmith, ‘Public Authority and Accountability in the Age of Transparency’, Australian Public Sector Anti-Corruption Conference (APSACC), Fremantle, November 2011.
³ Policing and Social Media, May 2012, Andrew Goldsmith, Katina Michael and Stuart Flynn.
1 Background

1.1 The Internet, the Web and Social Media

The internet is an indispensable component of 21st century life. It provides the infrastructure required to support a global computer network, enabling communication over that network via the use of agreed protocols for the transfer of information.

One of the main ways – but not the only way – to transfer information over the internet occurs via the web, using the HTTP protocol and HTML. While the terms ‘internet’ and ‘web’ are often used interchangeably, they are not synonyms. In this paper, ‘internet’ is used to refer to the underlying networking infrastructure, the foundation upon which the web has been built. The ‘web’ provides a way of enabling the transmission of information over the internet.

Of the many developments the web has witnessed over the past two decades, the recent emergence of social media stands out in terms of its impact and reach. Defined most simply, social media is any web-based environment that allows users to create, publish and share content easily. Social media is also described as ‘Web 2.0’.

On its face, the term Web 2.0 suggests a fundamental development in the web itself, but this is not the case. Rather, the term describes the user-focused, interactive and collaborative aspects of social media applications. One of its earliest proponents, Tim O’Reilly, describes it a concept with a ‘gravitational core’ rather than a ‘hard boundary’, a set of principles and practices that, taken together, describe the core competencies of the most successful web-based companies.

Web 2.0 has proved to be an incredibly popular term, quickly expanding to encompass a wide range of meanings. As a result, (somewhat retrospectively) it is possible to describe Web 1.0 as ‘connecting computers and making information available’, while Web 2.0 is about ‘connecting people and facilitating new kinds of collaboration’. So too, Web 1.0 can be used to describe static websites that lack interactivity and are proprietary, in contrast to social media/Web 2.0.

For Sir Tim Berners-Lee, the web’s inventor, Web 2.0 is a piece of jargon as, in essence, Web 1.0 was always already about connecting people and operating as an interactive space. As Berners-Lee notes, Web 1.0 also provides the foundation for Web 2.0 – the standards, the document object model, HTML, SVG, HTTP and so on.
However it is viewed, there is no doubt that in 2013 social media is firmly entrenched as a means of communication, online interaction and content generation. Initially adopted by individuals, businesses and government agencies too have embraced social media now. Social media has transformed the face of the web and its impact has been phenomenal. Facebook, for example, boasts more than 1 billion members worldwide, while those who choose not to participate can be described as ‘outliers’.11

A message to be drawn from this ongoing debate is that key terms and their meanings are not necessarily shared, thus clarity is required. In this report, the term ‘social media’ is used in preference to ‘Web 2.0’. ‘Social media’ is used to describe web-based applications only.

While the characteristics of social media websites are clearly compelling to individual users, this does not mean that they are appropriate for all possible uses or that they are neutral in their impact. In this report, the focus is upon the use of social media for law enforcement purposes; it is intended to be a constructive focus – identifying and assessing the opportunities, issues and risks as objectively as possible.

Finally, like the earlier manifestations of the web that came before it, social media is viewed with a degree of anxiety about the risks that it poses, which may be real, perceived or a mixture of both. This report seeks to identify where risks sit on the ‘anxiety continuum’, noting that perceived risks may be as destabilising as ‘real’ risks.

---

1.2 Social Media, Mass Communication and New Business Models

The shift from ‘old media’ (e.g. newspapers, television, radio) to ‘new media’ (e.g. social media) is often presented as a story of the *decreasing magnitude of power and control* that big business and government have held over the means of mass communication. It is argued that business and governments do not hold the privilege of exploiting, licensing, restricting access to, and managing new media as they did with old media.

Conversely, in this story, individuals and small groups are able to participate in mass communication using new media as never before. As a result, new media is viewed as a *democratising* force. For example:

- A single individual can communicate to the world if he/she wishes;
- Loose collectives of individuals can band together and exert considerable influence over businesses and governments; and
- Discrete topics or events have the capacity to ‘go viral’, reaching millions of people within a matter of minutes.

However this ‘story’ requires careful assessment. It is arguable that big business does – to a large degree – control new media (i.e. social media), albeit with the ongoing contributions of its individual users who either do not care or do not realise that this is the case.

The shift from old media to new media also signals a *new business model*. Under this model, *individual members* of social media do not need to purchase costly technology, physical distribution networks or (in the case of broadcasting) own a government licence. At the same time, it is social media members who produce the content that, in the past, was *paid for and produced by* media organisations. Almost uniquely, social media services do not pay for their content.

Participation in social media is based upon registration and, ordinarily, does not require a subscription fee or any other form of financial payment. Thus, while social media is built upon significant technical investment and innovation, this remains largely invisible to the individual member. This paper will suggest that *while participation in social media is ‘free’, it is certainly not without cost.*

Notably, social media providers also disclaim liability for large portions of their business operations. As a consequence of these disclaimers, responsibility for a range of legal issues is shifted to individual members instead. Social media services (largely US-based) operate their businesses *beyond the jurisdiction* of the majority of territories in which they operate (for example, Australia). In the event of any legal dispute between a social media service and an individual member the law of California is likely to prevail. *This business model raises a number of questions about the need to understand fully the risks and issues it poses.*

From a law enforcement perspective, under the terms of old media, law enforcement agencies have been able to oversee and react to old media reasonably effectively because its owners and controllers are few in number and clearly fall within the jurisdiction of local laws. With a decrease in the level of control – in particular, jurisdictional control – Australian law enforcement agencies have no advantage over social media owners, quite the opposite.

---

12 Using Google as an example, Tim O’Reilly notes that it is ‘delivered as a service, with customers paying, directly or indirectly, for the use of that service’ – ‘Google isn’t just a collection of software tools, it’s a specialized database. Without the data, the tools are useless; without the software, the data is unmanageable.’ [http://oreilly.com/web2/archive/what-is-web-20.html](http://oreilly.com/web2/archive/what-is-web-20.html)
1.3 **Examples of Social Media**

Social media enables individuals to create, modify, discuss and share internet content without writing code or using special tools.\(^\text{13}\) It has replaced old media’s ‘one-to-many’ business model with a ‘many-to-many’ media landscape encompassing a wide range of applications\(^\text{14}\) (see Figure 1, below).

![Figure 1 – Types of Social Media](image)

---


These types of social media work as follows:

- **Social networking sites** allow users to create a public profile that identifies their interests and the people they associate with on the site. Key examples include Facebook, LinkedIn and MySpace.
- **Online forums and discussion boards** allow individuals to post messages or comments for others to respond to. Key forums include the comments section of newspaper websites, Google Groups, Whirlpool and Facebook.
- **Blogs** allow individuals to make public ‘web log’ entries organised chronologically, for example, WordPress, Google Blogger and Facebook. Micro-blogs are small web log entries that are limited to small messages or notes, for example, Twitter, which enforces a 140-character limit.
- **Video and photo sharing websites** allow users to upload, view and discuss photos and videos. The most popular video and photo sharing sites are YouTube, Flickr, Instagram and Facebook.
- **Websites – such as Wikis** feature content that can be modified or contributed by users, for example Wikipedia and Facebook.
- **Video and podcasting** involve the serial publication of audio and video files, which may be subscribed to and downloaded through web syndication or direct streaming.
- **Online multiplayer gaming platforms** allow individuals to interact with each other through online gaming platforms connected via the web. Xbox Live and PlayStation are popular gaming platforms.
- **Geo tagging** allows users to publicly ‘tag’ themselves at a particular location, for example, Foursquare and Facebook.

While SMS is included in some definitions of social media, it is out of scope for the purposes of this issues paper as it is not web-based.

1.4 **Social Media’s ‘Ubiquity’**

Social media has become a staple tool of communication in contemporary society. Rather than meeting and communicating in person, conversations are increasingly occurring on social networking sites like Facebook, Twitter, MySpace and YouTube. Individuals are spending more and more of their time online, and establishing their public and private identities through cyberspace mediums.

The importance of the internet and social media as tools for the gathering and dissemination of information has also grown as the audiences for old media such as free-to-air television, newspapers and radio have dwindled and aged.

The prevalence of social media cannot be underestimated. In June 2012, Sensis reported that of Australia’s Internet users (98% of the population), 36% access social media sites once a day – 55% at least once a week or more. This figure is higher among younger users: 72% of people aged 20-29 accessed social networking sites at least once a day, as did 65% of 14-19 year olds. This use is on the rise – from 2011 to 2012, the percentage of internet users who accessed social media every day jumped a further 6%.

Victorians are amongst the highest users by state in Australia – of the 98% who access the internet, 43% of Victorians visit a social networking site at least once a day.
Facebook dominates at present as the most used social networking site, being used by 97% of Victorian social networking participants. This was unchanged from 2011. LinkedIn was a distant second most-used social media platform, attracting 16% of social networking users, up from 9% last year. Twitter was used by 14% of social networking site users, up from 8% last year, and Google+ was used by 8%.22

The level of engagement possible with the use of social media is startling. Facebook has more than 1 billion members worldwide, of which 11,808,360 members are based in Australia, amounting to more than 54.88% of the Australian population.23

While 94% of people use social media sites to catch up with friends and family, other reasons for their use are on the rise. For example, 27% of social network users used the sites to get information on news and current events, and 7% ‘to engage with a Government representative/Department.’24

Despite strong growth in social media usage, there are significant shifts in popularity of particular sites over short periods of time. Some 13% of Australian consumers who use social media reported that they had stopped using some sites, principally MySpace. Instagram, purchased by Facebook for $1 billion in April 2012, faced a backlash from its users in December 2012 when it announced changes to its privacy policy to make it easier for Instagram to share information with Facebook. Instagram has now postponed changes to its privacy policy until it has had time to explain them to users. In the meantime, a number of users have deleted their accounts.

At the moment, social media occupies the lead position in relation to web-based developments. However, discussion about ‘Web 3.0’ and/or the semantic web and what may come beyond Web 3.0 is already underway. While it is not possible to predict with any degree of precision what will eventuate, it is clear that the web will continue to evolve. Therefore, the current ‘ubiquity’ of social media needs to be considered in terms of the history of the development of the web. While social media is dominant now, it may not be in the future. After all, Netscape – a prototypical ‘Web 1.0’ company – did not survive the dotcom bust.

1.5 The Rise of Social Media in Law Enforcement

The huge growth in the use of social media is reflected in the amount of attention worldwide now being paid to its role in law enforcement. This includes a number of social media reports generated within law enforcement agencies, such as the UK National Police Improvement Agency’s 2010 report Engage: Digital and Social Media Engagement for the Police Service.25

In Australia, the Queensland Police Service has produced two outstanding internal reports: Disaster Management and Social Media – a Case Study (2011)26 and The Impact of New Media on the Queensland Police Service (2011).27

Social media/new media has also been a consistent theme at the annual Pearls in Policing28 conferences since 2010. In 2010, NSW Police Force Commissioner Andrew Scipione presented a paper on the challenges and opportunities for policing of modern communications

---

23 See http://www.socialbakers.com/facebook-statistics/australia
27 Review and Evaluation Unit, Inspectorate and Evaluation Branch, Queensland Police Service (2011). This is an internal QPS document and not publicly available.
28 Pearls in Policing is an international think tank conference dedicated exclusively to policing issues
technologies, particularly social media. In 2011, the conference considered the findings of a joint police-academic examination of the implications for law enforcement of the evolving nature of social media and associated new technologies. In 2012, the conference considered the findings of a working group, led by Commissioner Scipione, into an exploration of the pre-requisites for a global conceptual framework regarding the use of social media by law enforcement.

Just as telling of the growing importance of social media to policing has been the emergence of dedicated websites, such as:

- [http://www.connectedcops.net](http://www.connectedcops.net)
- [http://cops2point0.com](http://cops2point0.com)
- [http://www.iacpsocialmedia.org](http://www.iacpsocialmedia.org)
- [http://www.policesocialmedia.com](http://www.policesocialmedia.com)
- [http://thesmileconference.com](http://thesmileconference.com)

By way of example, ConnectedCOPS is a US private sector blog intended to:

> … enhance law officers’ ability to succeed with social media tools by providing insight, encouragement, education and the overall support required. It is also to promote the insightful thoughts of the law enforcement social media visionaries by providing them a voice…²⁹ (See below, Figure 2).

²⁹ ConnectedCOPS was founded and is directed by Lauri Stevens of LAwS Communications, who is also the founder and producer of the SMILE (Social Media in Law Enforcement) conferences and the COPPS (Citizens, Objectives, Plan, Policy, Schedule) social method for the development of social media policy for policing. [http://connectedcops.net/about/](http://connectedcops.net/about/)
ConnectedCOPS is a useful ‘one-stop-shop’ for sample social media policies and strategies, case studies, social media tools, tips, safety and publications, social media conference details and advertising for social media related products, in particular, law enforcement-related applications.

Another recent development has been the emergence of private sector, closed social media communities that are law enforcement specific. For example, CopBook is:

... an invitation only, secure collaboration environment that allows law enforcement officers to easily communicate on a social media-like platform on work related activities. CopBook users can interact on both an intra-department, and as elected, on an inter-department basis at the regional and/or national level with fellow members of the Public Safety and Law Enforcement community.

CopBook merges the roles of a standard PC intranet and a social media site. It allows members within a police force to create discussion groups to share information such as suspect locations and incidents and access documents such as policies, rosters, calendars, forms etc. It can also be configured to share information through discussion groups across jurisdictions and has an optional Community page, allowing members to share information with members of their local community.

While not strictly speaking within the scope of this paper, it is nevertheless worth noting the explosion in smartphone policing applications (apps), some of which may link to social media. These include:

- The UK Metropolitan Police app (find your nearest police station/street level crime map/emerging information/Twitter);
- Several US local sheriffs’ apps (providing police information, arrest reports etc., in real time);
- The Brooklyn Quality of Life app (reporting crime without having to go to police); and
- The New York Civil Liberties Union Stop and Frisk app (for use by witnesses of police stop and search incidents, particularly to report discriminatory or other inappropriate behavior).

There are also a number of commercially available apps for use on mobile devices such as Police Field Interview Card (which generates field interview cards and contact reports) and Police Pad (which keeps a detailed record of an officer’s shift recording log).

---

31 Example: Officer Safety: Survival Guide for Cops on Facebook.
32 http://www.efiia.com/content/three-efiia-creations-merge-new-information-sharing-alliance
33 A working demonstration of CopBook can be found at: http://www.youtube.com/watch?v=0a_Z8Y8iZak
2 Victoria Police

2.1 Background

Victoria Police was established in 1853 with 875 police officers. In 2011–12, Victoria Police had a total staff in excess of 16,000 people, including police members, public servants, protective security officers, forensic scientists and other specialists. It serves a community of more than 5.7 million people. This constitutes a particularly large police force, particularly in comparison with other jurisdictions (e.g. the UK, the US), where police forces are more fragmented.

Police services are provided at more than 500 locations across Victoria through 54 Police Service Areas (PSAs) split across 21 divisions within 4 Victorian policing regions. Victoria Police’s aim is to ensure that a safe and secure society underpins the economic, cultural and social wellbeing of Victoria with a focus on crime, public safety and road safety.

Victoria Police operates subject to a range of legislation, professional and ethical standards and policies. These provide the framework for the use and management of social media for policing purposes:

- **Legislation**: Victoria Police operates under the *Police Regulation Act 1958* (Vic). Additionally:
  - Binding data security and integrity standards were issued to Victoria Police in 2007 under the *Commissioner for Law Enforcement Data Security Act 2005* (CLEDS Act). The CLEDS Standards impose security and data integrity obligations on Victoria Police in relation to law enforcement data.
  - Victoria Police is subject to the *Information Privacy Act 2000* (Vic) and the *Health Records Act 2001* (Vic), except to the degree that law enforcement exceptions contained in both Acts apply in a given situation. It is noted that data security and data retention obligations continue to apply, as they are not included in the exception.
  - Victoria Police is subject the *Charter of Human Rights and Responsibilities Act 2006* (the Charter), which requires Victorian government agencies to adhere to, and uphold, human rights.

- **Professional & Ethical Standards**: The *Victoria Police Code of Conduct* provides the basis of Victoria Police’s professional practice and defines the expected standards of behaviour and conduct.

- **Victoria Police policies**: these are set out in the Victoria Police Manual Policies (VPMP) and the Victoria Police Manual Procedures and Guidelines (VPMG).

---

2.2 The Approach to the Use of Social Media by Victoria Police Members

Victoria has not enacted any social media legislation and social media is not specifically mentioned in the Police Regulation Act. However, specific reference to social media is found at the level of policy.

Victoria Police addresses both official and personal use of social media in its Social Media and Online Engagement Policy and other related policies. These policies are broadly consistent with legal obligations found in the CLEDS Standards and Victorian privacy legislation.

2.2.1 Official Use of Social Media by Victoria Police Members

‘Official use’ is defined as involving the use of social media tools acting as an authorised representative of Victoria Police.

When communicating via social media in an official capacity, employees must:

• Obtain authorisation from the Media and Corporate Communications Department
• Disclose themselves as a member of Victoria Police
• Comment only on information classified as public domain information
• Ensure content published is respectful and accurate
• Ensure they are not the first to make an announcement without authorisation
• Comment only on their area of expertise and authority
• Ensure the recipient has a legitimate business need for the information
• Adhere to the Terms of Use of the relevant social media platform and any other applicable laws.

Victoria Police employees are advised to be mindful of their safety, reputation and the reputation of the organisation when using online social networking sites. They are also advised to consider their privacy settings and to assess what information is placed on such sites, as their content may be accessed by an unintended audience and/or for unintended purposes.

The Recruiting Services Branch may use publically available information on social media to assist in making a determination on an applicant’s character and reputation.
2.2.2 Personal Use of Social Media

‘Personal use’ is defined as any use in a private capacity, whether using privately-owned or Victoria Police resources.  

Authorised users may use Victoria Police information systems to create, transmit or access public domain information provided that the use is incidental, occasional and does not interfere with work responsibilities, and constitutes a minor use of Victoria Police system resources.

When engaging in social media in a private capacity, employees must adhere to the Terms of Use of the social media platform and any other applicable laws. They must not:

- Make any comment about the administration of any Government department;
- Use Victoria Police email addresses or logos, disclose Victoria Police information, use the identity or likeness of another employee without consent, or post information that could be perceived as an official Victoria Police comment;
- Post or endorse any obscene, violent, discriminatory, vilifying, defamatory, offensive, insulting, threatening or harassing content;
- Publish material that might otherwise cause damage to Victoria Police’s reputation or bring it in to disrepute; or
- Access or use Victoria Police information, directly or indirectly, for private reasons or personal interest.

2.3 Victoria Police and ‘Digital Natives’

Based on the figures for Australian society in general, it is to be expected that the use of social media by members of Victoria Police is also significant, particularly in relation to ‘digital natives’.

‘Digital natives’ are individuals who have been immersed in digital technologies from birth and view integration with digital devices as the norm. It is calculated that approximately 72% of ‘digital natives’ access social media sites on a daily basis.

The demographic of ‘digital native’ within Victoria Police currently accounts for approximately 23% of members. If those on the cusp of being ‘digital natives’ are included – i.e. individuals 40 years old and under – this figure rises to 75% of Victoria Police members. It is estimated that 65% of Victoria Police members may use a social media site at least once a day.

It is also estimated that 85% of recruits into undercover agencies in Australia participate in social media and have an online profile. So too, the next generation of Victoria Police recruits (i.e. those aged 14–19 years) also demonstrate significant take-up of social media. The ability of these officers to participate safely in covert operations in the future is brought into question, as is the manner in which covert operations may be undertaken in the future.

---

46 VPMG Social Media and Online Engagement.
47 VPMP Access and Use of Information Systems.
48 VPMG Social Media and Online Engagement.
49 VPMP Access and Use of Information Systems.
50 Workforce at a Glance September 2012, Victoria Police intranet.
51 Workforce at a Glance September 2012, Victoria Police intranet.
52 Citing Mick Keelty in ‘Social media is changing the face of crime from the perspective of criminals, police and lawyers’ by Carolyn Ford, October 2012 88 (10) LJU p14.
It is clear that the generational changes taking place in Victoria Police will see growing use of social media as the preferred means of personal communication by members, as well as expectations that policing methodologies will utilise social media.

In early 2012, CLEDS conducted a survey of all sworn members of Victoria Police in order to assess the information security culture of Victoria Police. The survey found that 45% of all members regularly (at least once per week) use their own internet-enabled mobile phones for operational purposes. The figure rises to 88% of all members under 40 years of age.

Given the widespread use of social media in general, it is likely that a significant number of Victoria Police members are also using their own devices to access social media services for personal/unofficial purposes and, possibly, for semi-official purposes (e.g. to assist in their duties, but without prior authorisation).\(^{53}\)

In the following chapter, the ways in which Victoria Police (the organisation) uses social media to support its functions and activities are discussed in more detail.

---

\(^{53}\) CLEDS is currently conducting an ongoing program of site inspections of individual Victoria Police stations to test information security among uniformed members working ‘in the field’. As part of these site inspections, qualitative research will be undertaken into the degree to which officers use personally-owned devices, including their use to access social media.
3 Victoria Police & Social Media

As an organisation, Victoria Police uses social media for a number of its functions and activities, as illustrated below (see Figure 3).

![Figure 3 – Use of Social Media by Victoria Police](image)

3.1 Community Engagement

Victoria Police has an official social media presence on Facebook, Twitter, YouTube, and Blogspot. This enables Victoria Police to engage directly with the community in relation to information dissemination and crime prevention. Each social media presence operates differently, providing Victoria Police and its users with different functionality and levels of engagement.
3.1.1 Facebook

Victoria Police developed a Facebook page in 2004; it is used primarily to release information. With approximately 35,000 ‘likes’ in late January 2013, the page allows Victoria Police to reach beyond regular viewers of the Victoria Police News Page (www.vicpolicenews.com.au).54

The majority of posts are news articles that are automatically posted onto the Facebook page using the RSS feed of the Victoria Police News Page. Victoria Police uses the RSS Graffiti application. RSS Graffiti is a free service that allows users to periodically update one or multiple social network pages with any information feeds of their choosing.

As the administrators of the Facebook page, the Online Communications Unit adds links when new videos are added to the Victoria Police YouTube page or new posts are made on the Dandenong and Frankston blogs. Facebook users cannot post to the Victoria Police wall, but are able to ‘like’, comment and share on the stories that Victoria Police posts.

3.1.2 Eyewatch

In 2012, Victoria Police undertook a trial of Eyewatch, an online community engagement tool targeted at the regional level that uses the Facebook platform. The trial period ended in July 2012, with a review completed in December 2012.55 The review identified both positive and negative outcomes, but was inconclusive overall. It did find that Eyewatch has the potential to be effective particularly in ‘ethnically homogenous, low crime neighbourhoods with high levels of baseline confidence in police’.56 It recommends extending the pilot with an enhanced version of Eyewatch.

Eyewatch enabled local Police Service Areas (PSAs) to engage actively with the residents of a particular area, and anyone else who ‘liked’ the page, on issues relevant to that area. The trial involved Geelong, Hobsons Bay, Darebin, Brimbank, Yarra Ranges, and Public Transport Police Service Areas (PSAs).

PSAs were selected on the basis of two criteria:

- They represented areas identified as having significant policing challenges; or
- They represented areas identified as experiencing high police confidence.

The Eyewatch pages were set up in a consistent manner with similar types of information tailored to the specific area. All Eyewatch pages had Terms of Use, a ‘Meet the Inspector’ page, a map, and a link to the Crimestoppers web page (see next page, Figure 4).

Each participating PSO posted news and crime prevention information from local media, the Victoria Police Facebook Page and other Police pages (including NSW Police Eyewatch pages). The Eyewatch pages also uploaded CCTV photo captures or posted information regarding recent crime under investigation and where public support was required. The Yarra Ranges and Darebin PSAs used their pages to promote community engagement events such as the Bluelight Disco for under 18s or the ‘Little Red Car’.

The Eyewatch pages allowed users to ‘comment’ on each post as well as ‘share’ it with friends who may not follow the Eyewatch page. Users could also post questions, requests, general information, and suggestions (for public and police) to the Facebook wall. Users were required to post in accordance with the Terms of Use and warned they may be banned upon breach.

---

54 Victoria Police Facebook Page. Cf. NSW 171,000 likes, Queensland 319,000, South Australia 7,800, Western Australia 16,000.
55 The Victoria Police Eyewatch trial followed the trial and implementation of New South Wales Police’s Project Eyewatch, which commenced in mid-2011.
3.1.3 Twitter

Victoria Police uses its Twitter page as a tool to increase the reach of media releases from the Victoria Police News Webpage. It uses the RSS Feed from the News Webpage to post a new tweet periodically, with a link to the media release. Users are not able to read the story on Twitter due to limits imposed on the number of characters that may be utilised.

Other relevant posts about current events – such as traffic incidents, the Chief Commissioner’s appearance on radio, or major sporting events – may also be posted via Twitter.

3.1.4 YouTube

Victoria Police uses YouTube as a storage facility for publicly released video – ranging from news stories and CCTV footage, to public relations videos. The benefit of YouTube is that the videos stored there can be embedded easily onto other social media pages like Facebook and web pages.

The commenting features available on YouTube have been disabled, so users can only view and share videos without being able to comment on them. However, this does not prevent users from posting the video on their personal Facebook pages, forums, or blogs and commenting on those platforms.
3.1.5 Instagram

Instagram is the latest social media platform to gain significant popularity. It is a social network where members share images (often with effects built into Instagram) along with a caption. While still in its infancy, Instagram is viewed by Victoria Police as another tool for community engagement.

Victoria Police recently signed up to Instagram and links to it from Facebook (although, taking into account Instagram’s intention to change its TOU, this decision may need to be reviewed). The only other way for images to be seen is to access Instagram directly through a smart phone application. The images posted to date by Victoria Police are ones that had already been posted on its Facebook and blog pages with Instagram editing effects used.

3.1.6 Blogspot

There are two Victoria Police PSA blogs using Google’s Blogger site to publish localised blogs designed to engage and inform their communities. The ‘Dandenong, Casey & Cardinia Police’ (dandenongpolice.blogspot.com.au) and ‘Policing on the Mornington Peninsula’ (frankstonpolice.blogspot.com.au) blogs inform communities about the actions of police in the area, and seek feedback from the public to highlight issues that require greater police attention.

- The Dandenong, Casey & Cardinia Police blog features updates from the ‘Safe Suburbs Taskforce’. Formed in October 2011, the Taskforce is concerned with assaults and robberies in public places within the City of Greater Dandenong and City of Casey. The blog features information about the actions of the Taskforce as well as disseminating proactive advice to the public about going out in public places such as railway stations, parks, and licenced premises.

- The Mornington Peninsula Blog covers the Frankston and Mornington PSAs, and centres on the Community Response, Engagement and Social Tasking (CREST) strategy, and the Social Tasking Operations and Patrol (STOP) team. The STOP teams are the proactive policing teams tasked with addressing anti-social behaviour as part of the CREST strategy. As with the Dandenong, Casey & Cardinia blog, the blog posts are used to show the current efforts of the police in the region as well as providing the public with tips to minimise the risk of being victims of crime and anti-social behaviour.

Google’s blogger site allows members of the community to comment on each post, either using their profile or anonymously. To minimise the amount of moderation required, Terms of Use have been posted on each blog, providing users with an account of comments’ removal.

3.1.7 Wikipedia

Wikipedia is an online ‘public’ encyclopaedia that allows users to add, remove and revise entries in order to create a collaborative reference source. Since its creation in 2001, Wikipedia has expanded to a network of more than 77,000 active contributors, and has 470 million unique visitors each month.

Wikipedia is largely written by amateur volunteers; users with expert credentials are given no additional weight.57

---

The Victoria Police Wikipedia page began in October 2004 and has developed to contain in-depth information about Victoria Police’s historical background, ranking system and equipment used. It includes an image of the Victoria Police logo and motto. Victoria Police does not monitor the Wikipedia page. Information posted to Wikipedia consists largely of publicly available information obtained through existing sources.

The Wikipedia entry is also used on Facebook’s organisation page (as opposed to the official Victoria Police Facebook page), which provides Facebook users with information about an organisation based on its Wikipedia entry. This means the reach of the Wikipedia page is far greater than just the Wikipedia community (see Figure 5, below).

![Facebook Entry for Victoria Police](image)

**Figure 5 – Facebook Entry for Victoria Police**

### 3.2 Passive Intelligence and Criminal Investigation

The State Intelligence Division (SID) monitors social media. The Security and Organised Crime Unit within SID is currently trialling cyber-crime analysis software – Social Network Analysis Point Duty (SNAPD) – developed by a private sector provider. This software operates on publicly available information, providing an analysis of friendship networks. While this technology is in an embryonic stage – for example, it cannot assess the ‘strength’ of relationships or public sentiment – these are areas that could be developed in the future.
Information from social network sites is largely used to corroborate other intelligence. Where relevant, a ‘screen capture’ or a copy of text may be placed on a file. This information is not used as evidence. Where information contained on social media sites is required for evidentiary purposes, the file is transferred to the E-Crime Squad.

There is a ‘Chinese wall’ between the use of social media in SID for passive intelligence gathering and its use in the Crime and Undercover units for evidence gathering, to ensure correct procedures are followed within each of the departments.

### 3.3 E-Crime Squad

The E-Crime Squad is a major user of social media within Victoria Police and considers it to be an important tool for criminal investigations. Crime analysts access publicly available material to gather intelligence about persons of interest. The E-Crime Squad acts effectively as a central point for other Victoria Police units and commands in active investigations using social media.

### 3.4 Active Intelligence and Covert Operations

Several specialist units spread across Victoria Police undertake the active use of social media for covert operations. These units and their standard operational procedures cannot be identified as this has the potential to put such operations at risk.

It is noted that covert operational use of social media by Victoria Police is carried out by trained intelligence professionals and is unlikely to present any greater risk to Victoria Police and the members involved than standard covert operations.
3.5 **Internal Intelligence**

The Professional Standards Command (PSC) of Victoria Police uses social media sites (principally Facebook, although LinkedIn is also used for ‘profiling’) to:

- Investigate cases of Victoria Police members behaving inappropriately online (this usually involves members identifying themselves as police on social media sites and/or using such sites to openly discuss operational matters). Such cases are normally reported to PSC by third parties, rather than being the result of PSC actively seeking them out on social media sites;

- Formulate a profile of a target member under investigation (social media being just one of a series of tools used to formulate the profile); and

- ‘Integrity test’ suspect members.

PSC has four assumed identities for social media use. Currently, a single designated member of PSC is using one of the identities. The assumed identities were established in 2010 in accordance with the *Crimes (Assumed Identities) Act 2004* (Vic).

Rather than mask its IP addresses, PSC uses stand-alone computers to access social media sites. As a result, these computers cannot be traced back to the Victoria Police network.

3.6 **Recruitment**

The Victoria Police Recruitment Campaign uses social media as a marketing and information tool (see below, Figure 6). The Recruitment Services Branch (RSB) maintains the Victoria Police Recruitment Branch Facebook page, which currently has around 19,000 ‘likes’. Visitors to the page can ‘like’ it but not become a ‘friend’, which would open their Facebook profiles to Victoria Police.
The principal purpose of the recruitment branch page is to provide information to potential recruits/applicants regarding the recruitment process (for example, tips for interviews). It does not simply post information but rather invites potential recruits/applicants to post comments and ask questions, which are answered in sufficient time to maintain a dialogue. As such, the page acts as an efficient form of triage for potential recruits by answering pre-recruitment questions, such as whether having received a police ‘warning’ as a youth or having had driving offences in the past, are barriers to applying to join Victoria Police.

The Victoria Police Recruitment Branch Facebook page allows potential recruits/applicants to communicate with each and share their experiences about the recruitment process. Given the length of the recruitment process, this is a useful tool for maintaining interest in, and enthusiasm for, joining Victoria Police; it effectively creates an interactive community of potential recruits able to communicate with each other in real time. This could not be accomplished without social media.

The Recruitment Services Branch uses an assumed identity on Facebook to vet potential recruits, who consent to a full background check as part of the recruitment process. This is run from an account outside the Victoria Police system and involves access to publicly available information only. The assumed identity’s profile has privacy settings that prohibit access to the page; it makes no ‘friends’ and posts no comments.

### 3.6.1 Twitter Recruit

A further recruitment-marketing tool developed by Victoria Police, believed to be amongst the first of its type in the world, was ‘Twitter Recruit’, which took place over 23 weeks in 2010.

The purpose of ‘Twitter Recruit’ was for a Victoria Police recruit to share the experience of being at the Police Academy with the world (in particular, potential recruits) via Twitter.

Over the 23 weeks, a 21-year-old female recruit tweeted about her experiences at the Academy from 5 to 20 times daily. The recruit was provided with an iPad, trained in the use of Twitter and given guidance by the Victoria Police Digital Media Unit as to the tone and types of tweets that would be appropriate and effective. Otherwise, the recruit’s tweets were genuine and unscripted/unedited by Victoria Police. ‘@vicpolrecruit’ proved successful with over 1,000 followers in just two days.  

On occasions the recruit would also post YouTube video links shot with her during training and available at www.youtube.com/VPBlueTube. Links to the videos and the recruit’s profile were posted to the Victoria Police Recruitment Campaign website and the Victoria Police Recruitment Branch Facebook page.

Comments and questions received by the recruit over the course of the ‘Twitter’ campaign suggest that most followers were from Recruitment Branch’s target audience of people either already in the recruitment process or considering applying.

Recruitment Services Branch may undertake a similar campaign to support a Protective Services Officer recruitment campaign.
3.7 Enforcement

Where a Magistrate is satisfied that it is not reasonably practicable to serve a copy of an Intervention Order (including a Family Violence Intervention Order and a Personal Safety Intervention Order), the Magistrate may make an order for the document to be served in another manner. This may include service via Facebook, or other social media sites if deemed appropriate. Documents served via a social media site must be from an official Victoria Police Social Media profile, and the full details of the police officer serving the document must be provided. Victoria Police must also establish that the online location it is serving the document to is actually the respondent’s page/site.

This method of service has been used infrequently in Victoria.

3.8 Case Study: Piloting the Operational Use of Facebook

Up until now, Victoria Police has not sought to use social media fully for operational purposes. However, in December 2012, Victoria Police launched a pilot program involving Facebook at a suburban police complex.

The Facebook Pilot

The pilot was conducted over a period of two months and involved the use of a Facebook presence for operational policing, including intelligence gathering, crime investigation, sexual offence/child abuse cases and the execution of intervention orders.

The aim of the pilot was to assess which areas of operational policing could benefit from using Facebook.

The pilot used the Facebook private messaging system to send and receive messages from persons of interest, vulnerable persons, and provide access to any other page a Victoria Police member needed in the course of his/her duties. These messages were not publicly displayed on the Facebook ‘Timeline’ and remained private. Members were able to use the page to search other Facebook pages for information. Victoria Police members were instructed to not promote the Facebook page to individuals, groups, agencies, families and friends in the community as its focus was operational policing not community engagement.

The Officer-in-Charge was accountable for the implementation and management of the pilot Facebook page, and the monitoring of Victoria Police members’ use of Facebook in accordance with the pilot guidelines. The Officer-in-Charge was responsible for nominating the Administrators of the Facebook page.

The Administrators were the only employees authorised to communicate on behalf of Victoria Police on the Facebook page and have the authority and access to send private messages to other Facebook pages. The administrators were only identifiable to the Police Station avatar, but were instructed to identify themselves by name, rank and Victoria Police role when contacting other pages. As they were required to identify themselves, Administrators were advised to ensure that their personal Facebook pages had appropriate privacy settings so as to prevent unauthorised profile access.

The Media and Corporate Communications Department of Victoria Police managed the implementation of the project and provided assistance and support. A contact list was provided to the station with technical and support information. As the managers of the official, organisation-wide Victoria Police Facebook, Twitter, and YouTube pages, Media and Corporate Communications has broad practical experience with social media.

Victoria Police networked computers were used for the Facebook page and any communications through the Facebook account. Personal computers, mobile phones, iPads or other personal devices were not used.

59 See the Family Violence Protection Act 2008 (Vic) s.202, Personal Safety Intervention Orders Act 2010 (Vic) s 176.
60 So too, notification of court proceedings have been posted on social media sites, with further service of notice of proceedings and orders made via Twitter as well as (old-fashioned) email. http://www.claytonutz.com.au/publications/news/201012/24/st_kilds_nude_photo_social_media_scandal_leads_to_social_media_court_process.page
The findings of the evaluation of the pilot\textsuperscript{61} were inconclusive. This was attributed to limitations in the scope and implementation of the pilot which impacted negatively on its uptake by members. The evaluation also found that there were cultural issues at play which also explain the reticence of some members to use Facebook in an official capacity. The evaluation noted that there is an opportunity to conduct research into the cultural drivers that may influence members’ use of Facebook, which could ‘provide an understanding on what policing tasks could benefit from using social media such as Facebook as well as assist in the development of policy, guidelines, training and communication.\textsuperscript{62}

The evaluation report acknowledged that ‘there is a need from members to have official access to social media such as Facebook during the course of their duties’ and concluded that there is potential for the operational use of Facebook.\textsuperscript{63}

However the Facebook trial raises a number of legal, regulatory, privacy and policy issues that will need to be addressed and/or resolved prior to any further extension or enhancement of the pilot. These are discussed in more detail in the following chapter. At a minimum, the pilot provides a useful case study against which to consider compliance with information security, privacy and public records requirements as well as general Victoria Police policies and procedures.

\textsuperscript{61} Operational Use of Facebook (Pilot) Evaluation Report, Victoria Police April 2013

\textsuperscript{62} ibid

\textsuperscript{63} ibid
4 Issues, Benefits and Risks

4.1 Introduction

The weight of evidence accumulated through the researching of this report is clear: social media is neither novel nor a fad: the age of the monologue has given way to the age of the dialogue and, while the ‘social media revolution’ does not oblige participation, it is clear that the dialogue will continue without you if you choose to ignore it.64 The use of social media for law enforcement purposes is growing worldwide and it is apparent that social media has the capacity to be a wide-reaching and engaging law enforcement tool.

In Australia, social media has proved to be a useful source of intelligence and an effective tool for emergency management, community engagement and reputation management.65 At this point, social media has not become entrenched as an integral component of modern policing, although the Box Hill trial of Facebook for operational policing indicates it may have the capacity to do so in the future.66

In light of the current value of social media for policing – as well as its potential to expand further – it is important that social media issues and risks are understood so that any decisions by Victoria Police to adopt social media are both informed and subject to an appropriate risk-management assessment.

Law enforcement agencies recognise that in order to obtain the benefits of social media outcomes, they need to participate in social media and social networking platforms, most of which are decidedly more open and dynamic than they are accustomed to.67 However, unlike a member of the public, government organisations are subject to a range of legal and policy requirements that may not be consistent with social media usage and which need to be taken into account.

On the whole, the key determinants of social media’s benefits, dangers or risks in relation to law enforcement revolve around a number of factors including:

- The uses to which it is put;
- The manner in which it is deployed;
- Whether or not it is subject to an appropriate governance framework;
- Whether or not it is capable of complying with legal and regulatory requirements; and
- Whether the benefits it produces outweigh the risks.

This section of the report seeks to identify the major benefits, issues and risks posed by social media in a policing context. It is not intended to provide a comprehensive account of social media issues and risks, not least because it is beyond the scope of the report.68 However, it does seek to identify and group the most cogent issues and risks so that they may be subject to further analysis and review.

---

66 See section 3.8, above.
67 Jocelyne Bourgon, A New Synthesis of Public Administration: Serving in the 21st Century (McGill-Queen’s University Press), 2011, p.29. Indeed, this ‘openness and dynamism’ is one of the sources of social media issues and risks for government organisations.
68 In his publication, Legal Issues of Web 2.0 and Social Media, Stephen Kuncewicz notes that even when restricted to legal issues, ‘the subject matter of this report... is massive, and the definitions of many of the terms around which it revolves – social media, Web 2.0 – are fluid and open to question. The speech at which I can research and then type is not fast enough to keep pace with evolution.’ (Ark Publishing: London, 2010), p.XV. The updated version of this report, published in 2011, has already swelled from 232 pages to 303 pages.
4.2 Social Media Benefits

4.2.1 Social Media as a Source of Intelligence

Social media has the capacity to provide police with access to significant volumes of material, posted by all manner of people, and divulging astonishingly candid information to a public audience. This information is often contemporaneous with events of interest to police and can be documented and traced.69 Such information can prove to be a source of valuable intelligence, at times even capable of assisting in the pre-emption of crime.70 Increasingly, social media is used as a tool for gathering community intelligence that could be used to inform operational decision-making.

Analysis of social media content has been used to assist with offender apprehension and the location of missing persons.71 In addition, CSIRO has developed software to monitor and detect conversations related to fires, storms or floods on social media such as Facebook and Twitter, enabling early planning and intervention.72

Social Media as a Source of Intelligence

- In Queensland, police were able to locate seven witnesses to a murder case in a short period of time by uploading a Facebook post calling for information.
- In NSW, police charged two men with assaulting a taxi driver after a tip-off via Facebook.
- In Victoria, the launch of a campaign on Facebook elicited information from the public about the Gillian Meagher murder.
- In South Australia, police were able to locate missing persons using Facebook.

4.2.2 Emergency Management

Social media can enhance emergency management capability.73 Survey data collected from 1146 respondents in Australia and New Zealand showed that 75% would go to Facebook, and 31% would go to Twitter, as a communication channel should disaster occur.74 56% would rely on both social media and official sources for information about a disaster, and 52% indicated that they would post a request on a response agency’s Facebook Page if they could not get through on triple zero to the agencies.75

---

73 Emergency management refers to public emergencies, e.g. flood, bushfire or disasters of any sort, which are to be distinguished from personal emergencies. All social media platforms used by Victoria Police advise the public to call triple zero in the case of a personal emergency.
74 I M Taylor, G Wells, G Howell and B Raphael, ‘The role of social media as a psychological first aid as a support to community resilience building.’
75 Ibid.
Internationally, governments have published best practice guides for emergency preparedness, utilising social media prior to, during and after emergencies.76

In Australia, the benefits of using social media as a tool for emergency management were vividly demonstrated by Queensland’s experience of natural disasters in 2010.77

Following on from the success of social media use in Queensland, response agencies elsewhere in Australia have also created a social media presence.78

In South Australia, police recently launched new applications enabling smartphone users to receive live video streams of emergency bushfire updates.79 In Queensland, community members created Emergency 2.0 Wiki to provide a reference source on how to utilise social media effectively, in order to prepare, respond and recover from emergencies.80

4.2.3 Community Engagement

Social media has the capacity to transform the relationship between organisations and the community from one of command and control to one of collaboration and joint responsibility. For example, by engaging in two-way dialogue with government agencies through social media, members of the community are able to participate in their governing and contribute to the development of policies.81 Indeed, some view the rise of social media and social networking as:

... causing a ‘disruptive shift’ in the traditional balance of knowledge and decision-making power between government and citizens.82

---

76 See Social Media in an emergency: a best practice guide by New Zealand Government (30 June 2012), Use of social media in crisis communication (Belgium need to search), Project to advance crisis and emergency communications (Canada) and First Responder Communities of practice Virtual Social Media Working Group Community Engagement Guidance and Best Practices (US)

77 Queensland Police Services, ‘Disaster Management and Social Media – A Case Study’ 3: http://www.police.qld.gov.au/Resources/Internet/services/reportsPublications/documents/QPSSocialMediaCaseStudy.pdf. On the other hand, in 2010, Victoria’s experience of bushfires and social media was not so positive as social media platforms intended to provide fire information were overwhelmed with traffic and not loading. This is a particular problem in the country where internet capacity may be limited. In January 2013, as Gippsland experiences bushfires the Country Fire Authority’s smartphone and tablet application is continuing to malfunction, despite the release of a new version in December 2012.


80 http://emergency20wiki.org


This dialogue is seen as helping to create a resilient community, as members are able to raise their opinions and concerns directly, through participation.83

Law enforcement agencies need to maintain a high level of community trust and engagement, as effective policing is dependent on effective communication with the community. Law enforcement agencies communicate with the public for a variety of purposes, including the conduct of investigations and for educational campaigns.84 Social media presents an opportunity for agencies to connect with the general public, including traditionally disengaged community members, in a cost effective and efficient manner.85

4.2.4 Reputation Management

Social media provides an effective marketing tool for positive branding and reputation management. As Australians’ use of social media has increased, so too, a social media presence across small, medium and large enterprises has risen steadily over the past year.86 Of 1,016 individuals surveyed, 22% stated that they would use social media to find out about a particular brand or business, with 7% stating that they would use social media to engage with government representatives.87

Social media also provides an opportunity for law enforcement agencies to present themselves in a different light or engage with different types of people.88 Contact with law enforcement often occurs in a negative context, for example, filing a complaint or reporting a crime.89 Social media provides an opportunity for law enforcement agencies to interact with the community on a more positive basis.90

It has also been suggested that image work for police improves public perceptions, which, in turn, improves the effectiveness of police operational work.91

83 See M Anderson, ‘Integrating social media into traditional emergency management command and control structure: the square peg into the round hold’, presented at Emergency Media and Public Affairs Conference, 8 May 2012 for how social media help build a resilient community at time of emergency and crisis; See also http://www.police.nsw.gov.au/about_us/structure/operations_command/project_eyewatch on how local community could use social media to identify problems and help find a solution together.
85 The Victorian Project Eyewatch draft report states that one of the positive outcome of the project is that it provided the potential for the police to communicate with members of the community who may have otherwise never interact with law enforcement agents, particularly youth. The NZ Policing Act wiki reached a number of people who would otherwise not participate in policy development: http://www.police.govt.nz/news/release/3370.html
87 Ibid.
88 The Victorian Eyewatch draft report states that one of the positive outcome of the project is that it provided the potential for the police to communicate with members of the community who may have otherwise never interact with law enforcement agents, particularly youth.
89 http://connectedcops.net/2011/06/21/breaking-news-from-the-law-enforcement-newsroom/
4.3 General Legal & Regulatory Issues

As a starting point, no one is likely to disagree with the statement that social media raises legal and regulatory issues. However, it is just as likely that a broad and – at times – inconsistent set of reasons are given for this state of affairs.

This section of the paper seeks to outline the key legal issues that may arise when social media is used for law enforcement purposes. It is intended to demonstrate that:

- Social media raises a number of general legal and regulatory issues for Victoria Police, as well as some that apply specifically to Victoria Police; and
- On the whole, it is clear that offline laws apply equally to the online world.92

The following discussion does not attempt to provide a detailed assessment of the legal environment. It is presented with the caveat that when social media is used for law enforcement purposes, the legal implications must be viewed seriously as the consequences of ‘getting it wrong’ are grave (both in terms of law enforcement and reputation).

4.3.1 Social Media Terms of Service

In Australia, the way in which contracts are formed and the rules that govern their validity are largely derived from the common law.93

In legal terms, social media is based on contract law with the use of a social network platform generally governed by the service's Terms of Use (TOU). In cases where the TOU do not apply or are inadequate, the relationship between the subscribing party and the platform provider will be governed by general law principles.94

The contractual arrangement with social media services are most often effected through ‘click-wrap’ contracts and are usually non-negotiable.95 The US Second Circuit District Court has described click-wrap arrangements as:

A click-wrap license presents the user with a message on his or her computer screen, requiring the user manifest his or her assent to the terms of the licence agreement by clicking on an icon. The product cannot be obtained or used unless and until the icon is clicked.96

The validity of click-wrap online contracting in Australia was reviewed and upheld by the Federal Court of Australia in eBay International AG v Creative Festival Entertainment Pty Ltd.97

---

93 There are a number of exceptions. Some contracts must comply with statutory requirements, including consumer credit contracts, contracts for the disposition of interests in land and copyright assignments and exclusive licences.
94 Similarly, a court may choose to apply general law if they determine that it overrules or contradicts the TOU. See QUT Legal Aspects of Web 2.0 Activities (2007).
96 Specht v Netscape Communications Corp, 150 F Supp 2d 585.
The social media services used by Victoria Police set out general terms and conditions within their TOU, Privacy Policy and/or Community Standards. The terms and conditions are broadly consistent across all platforms and inevitably favour the service:

*The user agrees to comply with certain ‘rules of engagement’ with regard to conduct and the site operator excludes all liability and reserves the right to remove any content that it deems inappropriate.*

The following table provides a summary of social media TOU. The TOU are generally consistent across all platforms used by Victoria Police.

<table>
<thead>
<tr>
<th>The TOU commonly:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Disclaim the provider’s liability for a user or third party’s usage and provision of content and information onto a site.</td>
</tr>
<tr>
<td>• Provide an indemnity for the provider against any loss, damage or claims arising from the use of the service or breach of the agreement.</td>
</tr>
<tr>
<td>• Obtain a warranty from users that any uploaded material does not breach the legal rights of any other person, including copyright, contract and privacy rights.</td>
</tr>
<tr>
<td>• Allow the provider to remove uploaded content for reasons stated in the terms, usually due to breach of terms or copyright infringement.</td>
</tr>
<tr>
<td>• Allow the provider to unilaterally alter the terms with or without notice, and with or without opportunity for the users to comment.</td>
</tr>
<tr>
<td>• Allow the provider to terminate the account with or without notice, usually due to breach of terms or repeated copyright infringement.</td>
</tr>
<tr>
<td>• Allow the service provider unfettered licence to use any intellectual property content posted on the site. This licence remains until the account is terminated, unless the content has been shared with others and not removed.</td>
</tr>
<tr>
<td>• Apply the law of the State of California should any dispute arise between the service provider and the user.</td>
</tr>
</tbody>
</table>

98 The terms and conditions are labelled differently in each platform. Facebook labels them as Statement of Rights and Responsibilities, Data Use Policy and Community Standards; Twitter labels them as Terms of Service, Privacy Policy and Twitter Rules; YouTube labels them as Terms of Service, Privacy Policy and Community Guidelines; Google Blogspot labels them as Policies & Principles which comprise of Privacy Policy and Terms and Instagram labels them as Terms of Use, Privacy Policy and Terms of Use for Instagram API. YouTube shares a Privacy Policy with Google Blogspot.


100 Facebook Statement of Rights and Responsibilities clause 16(2) & (3); Twitter Terms of Service clause 11 Part C and clause 4; YouTube Terms of Service clause 5d and Google Terms of Service under Warranties and Disclaimers and Instagram Terms of Use do not contain equivalent term.

101 Facebook Statement of Rights and Responsibilities clause 16(2) & (3); Twitter Terms of Service clause 11 Part C and clause 4; YouTube Terms of Service clause 9; Google Terms of Service under Liability for Our Services and Instagram Terms of Use do not contain equivalent term.

102 Facebook Statement of Rights and Responsibilities clause 5; Twitter Terms of Service clause 5; YouTube Terms of Service clause 6D and Instagram Terms of Use under Proprietary Rights in Content on Instagram clause 3.

103 Facebook Statement of Rights and Responsibilities clause 5 and 8; Twitter Terms of Service clause 9; YouTube Terms of Service clause 6F and 7; Google Terms of Service under Modifying or Terminating the Terms and Instagram Terms of Use under General Conditions clause 5.

104 Facebook Statement of Rights and Responsibilities clause 1 and 14; Twitter Terms of Service clause 1; YouTube Terms of Service clause 1B; Google Terms of Service under Modifying or Terminating the Terms and Instagram Terms of Use under General Conditions clause 2.

105 Facebook Statement of Rights and Responsibilities clause 5(6); Twitter Terms of Service clause 1 and 9; YouTube Terms of Service clause 7; Google Terms of Service under Modifying or Terminating the Terms and Instagram Terms of Use under General Conditions clause 1.

106 Facebook Statement of Rights and Responsibilities clause 2(1); Twitter Terms of Service clause 5; YouTube Terms of Service clause 6C; Google Terms of Service under Your Contents in Our Services and Instagram Terms of Use under Proprietary Rights in Content on Instagram clause 1.

107 Facebook Statement of Rights and Responsibilities clause 16(1); Twitter Terms of Service clause 11 Part B; YouTube Terms of Service clause 14; Google Terms of Service under About these Terms and Instagram Terms of Use do not contain equivalent term.
While these terms and conditions provide a framework for assessing disputes between a user and a social media service, they do not include third parties because of privity of contract issues and cannot be used to determine disputes between users. Instead, conflicts between users rely upon general legal remedies such as copyright infringement or defamation. As the TOU shift many legal responsibilities to users, this raises the risk that a user (i.e. Victoria Police) may be held responsible for the actions of a third party.

An issue of widespread concern to many users of social media is the practice of service providers unilaterally changing the TOU. One of the most controversial recent examples was Instagram’s attempt in December 2012 to change its TOU which aimed to confer users’ intellectual property rights on Instagram. The proposed changes included this clause:

_Instagram does not claim ownership of any content that you post on or through the service. Instead, you hereby grant to Instagram a non-exclusive, fully paid and royalty free, transferable, sub-licensable, worldwide licence to use the content that you post on or through the service, except that you can control who can view certain of your content and activities on the service as described in the service’s Privacy Policy._

One of the main effects of the amendment was to permit Instagram to commercialise user content without the consent of, or compensation to, users.

The proposed changes caused a storm of protests. Many users removed their content and deleted their accounts. Although Instagram backed down in this case, it is a frequent occurrence for service providers to amend contractual terms with little notice to users and for purposes designed to benefit the service provider. Amendments to TOU often have a retrospective effect, a case in point again being Instagram. The content licensing changes it sought to impose were not confined to content posted by users after they came into effect – they applied to content posted before the TOUs were changed.

The very real prospect of unilateral changes to TOUs and their potential to significantly affect the legal basis of the arrangements between service provider and user carries with it governance, risk management and resourcing issues for Victoria Police. A variety of Victoria Police Departments and operational units use social media. Each establish its own relationship with social media platforms. Some are better resourced than others to monitor and assess the impact of changes to TOUs and, in each case, risk assessment needs to take account of the particular circumstances applicable to operational circumstances. In the absence of an overarching governance framework, there is a significant likelihood that responses to TOU issues will be fragmented and that police resources will not be used effectively.

A British online retailer, Gamestation, amended its contractual terms and conditions to include:

_By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant us a non-transferable option to claim, for now and for ever more, your immortal soul. Should we wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorised minions._

_We reserve the right to serve such notice in 6 (six) foot high letters of fire, however we can accept no liability for any loss or damage caused by such an act._

The updated terms and conditions were an April Fool’s joke designed to illustrate a serious point: almost no one reads online terms and conditions and organisations are free to include whatever language they want. Almost 90% of customers didn’t read the amended terms and conditions.*

4.3.2 Jurisdiction

As discussed earlier (section 1.2, above), the issue of jurisdiction is significant. It raises both legal and practical issues for Victoria Police. Should Victoria Police need to take action against one of its social media providers, it will most likely take place in California and subject to Californian law. This raises issues about the differences between Australian and US laws as well as the practical issues associated with being represented overseas. The degree of risk and difficulty of acting both need to be taken into account in any risk management assessment.

The Wikipedia entry for Victoria Police illustrates a number of these issues via its reproduction of the Victoria Police logo (shield and motto). Wikipedia recognises that the logo is subject to copyright, providing an online statement to justify its use:

This is a logo of an organisation, item, or event, and is protected by copyright. It is believed that the use of low-resolution images on the English-language Wikipedia, hosted on servers in the United State by the non-profit Wikimedia Foundation, of logos for certain uses involving identification and critical commentary may qualify as fair use under United States copyright law. 

Wikipedia relies upon jurisdiction to assert this claim. Leaving aside whether or not the logo is low resolution, its use assures readers that ‘they have reached the right article containing critical commentary about the organisation, and illustrate the organisation’s intended branding message in a way that words alone could not convey.’ As outlined below, at section 4.5.4, Victoria Police members have taken issue with the Wikipedia ‘critical commentary’ as it is perceived to be inaccurate and biased. In this context, use of the logo adds (questionable) authority to the content.

In 2002, the High Court of Australia ruled that an Australian plaintiff could sue for defamation in Australia, where the material was downloaded, even though the publication occurred in the US. More recently, an Australian lawyer attempted to sue the US-based Twitter on behalf of his client. These cases highlight the complexity of jurisdictional issues.

More recent comments on this case note that, after ten years of ongoing online developments – in particular, social media – there is still insufficient clarity in relation to the respective liabilities of servers and social media ISP providers, although the primary concern remains the ‘lightning fast’ dissemination of information via social media and the impossible task of ‘getting it back’.

4.3.3 Social Media and Criminal Investigations

Social media is used to arrange and execute crimes. Information posted on and communicated through social media sites is becoming increasingly important to Victoria Police in undertaking its law enforcement activities.
The problem posed by social media for criminal investigations is that relevant information is held by foreign enterprises, often domiciled in the USA without an office within Australia, and in cloud-based computer servers that could be located anywhere. Conventional policing methodologies, which rely on powers of search and seizure, simply do not apply in these circumstances.

Australia has in place a framework, developed under the Mutual Assistance in Criminal Matters Act 1987, known commonly as ‘mutual assistance’ which establishes a ‘process countries use to obtain government to government assistance in criminal investigations and prosecutions.’ The mutual assistance legislation operates in conjunction with international law, including a number of bilateral mutual assistance treaties to which Australia is a party. Under the mutual assistance framework, Victoria Police, through the Commonwealth, is able to seek and obtain information from foreign countries relevant to criminal investigations. However, the process takes time, can be cumbersome and was not designed to support international criminal investigations and intelligence gathering in today’s global information environment.

Time is of the essence in many criminal investigations and Victoria Police’s operational capabilities are hampered by its practical inability to access, in accordance with due process requirements, social media content that could assist its investigations. The process is somewhat simpler where social media services have a presence in Australia but there are numerous examples where their lack of cooperation has frustrated law enforcement.

There is thus a gap in Victoria Police’s ability to obtain timely access to material on social media sites for investigatory purposes. There is a clear need for it to establish arrangements with social media services who operate in Australia to remedy this situation. That said, it is difficult to envisage that this could be done without the assistance of, and leadership from, the Commonwealth given that it has Constitutional responsibilities for external affairs and telecommunications and has the legal and administrative responsibilities described earlier in relation to mutual assistance. Addressing these issues is a national responsibility.

The most controversial example of this concerns the murder of Jill Meagher in Melbourne in September 2012. Social media featured prominently: a ‘Help us Find Jill Meagher’ group was established to attempt to locate her in the hope of finding her alive. In the space of a few days it attracted more than 120,000 likes. Many other groups were established along similar lines and provided information to authorities.

After Ms Meagher’s body was found and a suspect arrested, social media became a focus for public reaction to the point that authorities became concerned about the potential for trial by social media and thus prejudicing the suspect’s right to a fair trial. Victoria Police attempted to persuade Facebook to remove the offending material. Facebook refused:

---

**Laws affected by social media**

- Defamation
- Intellectual property
- Copyright
- Evidence
- Privacy, confidentiality, secrecy
- Racial vilification
- Sexual discrimination & harassment
- Offensive or obscene material
- Contempt of court
- Crimes

---

Victoria Police Chief Commissioner Ken Lay has told Fairfax Radio that Facebook will not cooperate in removing the page and he is seeking legal advice.

“Though social media’s been enormously helpful in this investigation, it’s also been very, very difficult and we had cause to speak to Facebook over the weekend and ask them to take a particular site down,” he said.

“Now, they’ve refused to do that. We’ve all got a social responsibility. Facebook is part of our community and I would have thought that it would have only been reasonable.”

### 4.3.4 Social Media’s Impact on Other Laws

As a matter of course, any organisation using social media services to communicate with the public or to promote itself, or allowing its employees to use social media needs to take account of a number of specific laws (see text box, below).

Each of these laws applies now to the offline world and ‘Web 1.0’. While egregious recent examples of ‘trolling’ in Australia resulted in populist calls for additional legal protection against social media ‘trolls’, it is clear that existing laws are capable of dealing with many categories of social media abuse (see Figure 7, below).

<table>
<thead>
<tr>
<th>Menace, harass or cause offence</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The intention of committing a serious offence</td>
</tr>
<tr>
<td>• To make a threat</td>
</tr>
<tr>
<td>• To make a hoax threat</td>
</tr>
<tr>
<td>• To menace, harass or cause offence</td>
</tr>
<tr>
<td>In 2011, Bradley Hampson became the first person to be prosecuted and jailed for trolling under section 474.17 of the Criminal Code.</td>
</tr>
<tr>
<td>The Queensland Police Service Computer Crime Team was able to identify Hampson despite his messages to a Facebook tribute page being anonymous.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contempt of court</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covers the publication of material – including through social media – that may have a tendency to prejudice pending court proceedings (especially material that will not form part of the evidence).</td>
</tr>
<tr>
<td>Most recently the Jill Meagher case provoked an outpouring of information about the man charged with her murder. Victoria Police used Twitter to inform tweeters that posting comments endangering the presumption of innocence can also jeopardise a trial. Many commentators also pointed out that ignorance is not a defence to defamation, libel or sub judice.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inducing/inciting violent behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>In September 2012, NSW police charged two men with ‘recruiting persons to engage in criminal activity and printing/publishing to incite/urge/aid commission of crime’ via social networks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defamation</th>
</tr>
</thead>
<tbody>
<tr>
<td>In 2012 in South Australia, a 19-year-old was charged with criminal defamation for setting up a Facebook Group called ‘Piss off Mark Stuart’ about a local Senior Constable.</td>
</tr>
<tr>
<td>The Group contained posts from other contributors that were found to be incorrect, offensive and grossly defamatory. The page was active for 4 to 5 days before it was taken down.</td>
</tr>
<tr>
<td>The creator of the page was placed on a two-year $500 good behaviour bond.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google was found to have breached the <a href="http://comlaw.gov.au">Privacy Act 1988 (Cth)</a> when it collected data – including personal information – from unsecured Wi-Fi networks via its Street View cars. Google undertook to destroy any personal information that was collected in 2010.</td>
</tr>
<tr>
<td>However, in 2012, further data was identified and was subsequently deleted.</td>
</tr>
</tbody>
</table>

---

It is important to remember that the potential for many of these laws to impact negatively upon an organisation now are covered by existing organisational policies and procedures. In many instances, these policies and procedures can be/have been extended and/or applied to social media use.\textsuperscript{117} Taking these steps also functions as a form of risk management, particularly if it is accompanied by staff training.

Otherwise:

- To the degree that social media represents a novel use of technology it may not be clear how the law applies in the short term, resulting in ambiguity or anxiety about ‘getting it wrong’. While this may require careful consideration, more often than not current legal arrangements will be capable of applying.

- In the event that genuine legal problems are identified, legislation may be developed in response.\textsuperscript{118} Otherwise, new technology-specific ‘social media legislation’ may be proposed on public policy grounds in order to provide confidence or to confirm that a law applies.\textsuperscript{119}

- Finally, social media commentators vary widely in terms of their legal expertise. In some cases they adopt the role of ‘bush lawyer’ and despite questionable interpretations, these are taken up with great enthusiasm by followers, inspiring others to share their misrepresentations of the law.

Overall, while the laws listed above may present hazards and should not be ignored, most often they are amenable to risk management and, where appropriate, accounted for in organisational procedures and policies.

4.3.4.1 Intellectual Property

The main intellectual property issue for law enforcement agencies is copyright. The owner of copyright in a work or other copyright subject matter has the exclusive right to exercise the rights comprised in the work or other subject matter. Thus, if Victoria Police wishes to post copyright material to, or utilise copyright material from, a social media site, it must take care not to infringe copyright.

Frequently social media services require users to provide the service with some form of copyright licence that covers the material the user uploads to the site. Often the licence is accompanied by a clause which requires the user – i.e. Victoria Police – to indemnify the service provider from any copyright infringement claims. Clearly there is a need for proper copyright management policies to be implemented by any law enforcement agency using social media.

\textsuperscript{117} See, for example, the social media policies produced by the State Services Authority, Department of Justice and Victoria Police: http://www.ssa.vic.gov.au/images/stories/product_files/442_PSSC_Social_Media.pdf; http://www.justice.vic.gov.au/home/about+us/our+values+and+behaviours/social+media+policy/ and VPMG, Social Media & Online Policy.

\textsuperscript{118} See, for example, Michael Endler, ‘California passes tough social media privacy laws’, Information Week (1 October 2012): http://www.informationweek.com/security/privacy/california-passes-tough-social-media-pr/240008206. The US approach to privacy regulation tends to follow a technology-specific or subject-specific approach, rather than the more comprehensive approach taken in the Asia Pacific and Europe: the US law prevents employers from requiring access to prospective employees’ private information held on social media sites, a scenario that has not arisen in Australia. The unexpected impact of the Victoria Sexual Offenders Register legislation upon teenagers caught ‘sexting’ provides a good example of a mismatch between law and technology/public policy.

\textsuperscript{119} To a large degree, Australia’s national Electronic Transactions Act framework was enacted in order to assure confidence and trust in the use of electronic transactions, including electronic signatures (where not specifically excluded under law).
Intellectual property risks are also linked to service provider terms and conditions in another way. The service provider can amend the terms of service virtually at will and without a great deal of notice, as was the case of Instagram (see section 4.3.1, page 32).

4.3.4.2 Privacy

The question whether a social media company that has no Australian business presence is regulated by the Privacy Act 1988 (Cth) is currently unclear. Due to the operation of the extra-territorial provisions of the Privacy Act 1988, the analysis of whether a social media company has obligations under privacy legislation will depend on the individual facts and circumstances.

The Privacy Act 1988 (as amended by the recent Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)) extends to an act or practice engaged in outside Australia by an agency, or where the organisation has an ‘Australian link’ (section 5B(1)). An organisation or small business operator has an Australian link if:

- it is an Australian citizen;
- a person whose continued presence in Australia is not subject to a limitation as to time imposed by law;
- a partnership, trust or body corporate formed in Australia; or
- an unincorporated association with its central management and control in Australia (section 5B(2)).

An organisation or small business operator also has an Australian link if an organisation or operator ‘carries on business’ in Australia, and if the personal information was collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice (section 5B(3)).

Part V of the Privacy Act 1988 (i.e. the Privacy Commissioner’s complaint functions) has extra-territorial operation, meaning that the Privacy Commissioner can initiate and investigate complaints overseas where the above subsections are satisfied (section 5B(4)).

Accordingly, whether a social media company is ‘carrying on business’ in Australia, or whether information is ‘collected or held in Australia’, even if the information is eventually stored offshore, is unclear and would likely turn on the facts and circumstances. The phrases ‘carrying on business’ and ‘collected or held in Australia’ have not been considered in depth under the Privacy Act 1988, but do exist in other contexts (such as the former Trade Practices Act 1974 (Cth), which also contains the phrase in an extra-territorial context). This makes it difficult to determine decisively whether or not social media is bound by the Privacy Act 1988.

---

120 In Bray v F. Hoffman-La Roche Ltd [2002] FCA 243, in the context of the Trade Practices Act 1974 (Cth), the Federal Court consider that whether or not a body corporate is ‘carrying on business’ is to be assessed at the time of the alleged contravention of the TPA.
Although it is likely that a social media service that has an Australian office or presence comes within the jurisdiction of the *Privacy Act 1988*, for social media companies that do not, section SB raises jurisdictional issue that need to be determined before any action could be taken by the Australian Privacy Commissioner. In this regard, issues regarding the nature and extent of the social media service’s Australian operations will be significant. Social media services TOU typically include intellectual property licensing provisions. These could be conceptualised as the systematic and widespread practice of trading in intellectual property in return for the provision of services and may thus underpin an argument that these activities constitute ‘carrying on business’ to an extent that is sufficient to bring them within the operation of the *Privacy Act 1988*.

### 4.4 Specific Regulatory Issues

There are two areas of regulation that warrant specific consideration:

1. Victoria’s public records framework under the *Public Records Act 1973* (Vic)
2. Victoria Police’s information security framework under the *Commissioner for Law Enforcement Data Security Act 2005* (Vic) (CLEDS Act)

#### 4.4.1 Victorian Public Records and Social Media

Under the *Public Records Act*, recordkeeping standards have been issued to the Victorian public sector. These standards apply to the creation, control, storage and disposal of public sector records.

The *Public Records Act* defines a public record as ‘any record made or received by a public officer in the course of [their] duties’. It does not define a record according to its format, but rather its content. Thus, records created as a result of using social media are subject to the same business and legislative requirements as records created by other means such as in a document or in a database, during formal or informal meetings, in emails or telephone file notes.

In November 2012, the Public Record Office Victoria (PROV) released *The Recordkeeping Policy: Social Media*. The policy was developed following the earlier release of an issues paper and associated consultation period and is intended to remove any confusion as to whether or not the use of social media results in the creation of ‘records’. The social media policy states that:

- Public officers *create records* when using social media as part of their duties
- Requirements for record creation, control, storage and disposal contained in the PROV Recordkeeping Standards *are not media-specific* and apply to social media
- Records resulting from social media use *must be captured* in a timely manner, as it is not guaranteed that they will remain available, even in the short term.
- Records must *preserve the context* in which the social media usage was made
- The policy covers *metadata, privacy and disposal* in relation to records of social media use.

---

As this summary illustrates, when Victoria Police uses social media, it will result in the creation of public records. The record-keeping requirements arising from Victoria Police’s use of social media are likely to be significant and will require compliance measures to be developed, at least in the short term (see also, section 4.4.2 below).

However the management of social media records and data retention is a more complex issue than the PROV social media policy suggests. Government agencies such as police have no control over primary data retention, which is in the hands of the social media service providers. As the use of social media by law enforcement agencies and government in general increases, the task of making and storing secondary copies of public records created on the media becomes onerous to the point of physical impossibility. Reliance will ultimately be on the prime data held by the service providers. Law enforcement agencies will need to assess the expectations they reasonably have of service providers in terms of data storage and retention. They will also need to address the issue in maintaining social media records of how the data can be made easily accessible so it can be used effectively and efficiently for law enforcement.

Further work is required to assess the full impact of social media in relation to Victoria Police’s record-keeping requirements. At a minimum, a response to the PROV social media policy will need to be documented within Victoria Police.

4.4.2 CLEDS Act & Standards

Victoria Police must comply with Standards for Victoria Police Law Enforcement Data Security 2007 (CLEDS Standards) issued under the CLEDS Act. The CLEDS Standards distil a number of international and national information security benchmarks into one document. They ‘constitute a comprehensive set of information security obligations that bind Victoria Police and against which they are accountable.’ Overall, the CLEDS Standards outline:

[T]he necessary controls for the secure management of law enforcement data systems and the information they contain. They also incorporate best practice to be observed in relation to law enforcement data security management.

Compliance with the CLEDS Standards enables Victoria Police to maintain the confidentiality, integrity and availability of law enforcement data. Records created through the use of social media are ‘law enforcement data’ for the purposes of the CLEDS Act and are, therefore, subject to the CLEDS Standards in the same manner as any other law enforcement data.

In general, the Standards relating to ‘release’ (meaning any disclosure of law enforcement data) raise a number of compliance issues, as any engagement with social media services will result in the disclosure of law enforcement data to the social media service provider (at a minimum). See, for example:

- Standard 11: release of law enforcement data must only occur if that disclosure is authorised
- Protocol 11.3: release must be monitored and logged
- Protocol 11.5: recipients must be made aware of their responsibilities when receiving law enforcement data.

127 CLEDS, Annual Report 2008-09, p.10. The Victorian Government also takes a WOVG view of IT security, mandating that Victorian Government departments and agencies – including Victoria Police – must adhere to WOVG information security policy standards and guidelines. On the whole, these are articulated at a lesser degree of detail than the CLEDS Standards. If there is a conflict between the two approaches, the CLEDS Standards prevail: https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security-sec-std-information-security-management-framework
Social Media and Law Enforcement

- Standard 12: law enforcement data passed to members of the public and other third parties via electronic messaging (including email) must be appropriately protected.
- Standard 13: disposal of law enforcement data must be authorised and occur in a timely fashion.

In particular, the Box Hill Facebook pilot involving the use of Facebook’s private messaging system for operational policing purposes raises a number of questions in this respect. While there is insufficient space to consider all of these in detail, as a starting point, consider:

- How is it possible to maintain the confidentiality of Victoria Police data as any law enforcement data passing through the Facebook private messaging system is viewable and, potentially, useable, by Facebook?
- How can destruction requirements be met when Facebook retains data permanently?

In essence, Victoria Police experiences a loss of control over Victorian law enforcement data when using Facebook private messaging for operational purposes.

Further work is required to assess the full impact of social media upon Victoria Police’s compliance with the CLEDS Standards.

4.5 Control

Perhaps the major issue law enforcement agencies must confront in adopting social media as a contemporary policing tool is lack of control. This is particularly difficult for organisations such as police which are used to being ‘in control’, of which the very structure and culture is one of ‘command and control’.

While law enforcement agencies can define the terms of their own engagement and exercise a degree of control over the online behaviour of their own members, through policy, education and training, they have no control over the behaviour, protocols and expectations of the broader online community using social media. People’s tendency to act with less circumspection online than in the physical world is an advantage to police when gathering intelligence, but throws up considerable challenges for effective community engagement and reputation management.

Law enforcement agencies – and government in general – need to be fully aware when using social media that these are mediated services. Real control in social media is not exercised by the users, for as ‘democratic’ as contemporary folklore may have it, but by the service providers. These providers are in most cases private entities, located in jurisdictions beyond the control of Australian law enforcement agencies and who set their own terms of use. They wield considerable power and the power balance between them and government and its agencies, such as police, is definitely in their favour.

This section of the report outlines some areas where this lack of control poses major risks for law enforcement agencies. As traditional control is not possible, these risks need to be faced by law enforcement agencies, analysed and effectively managed. That in itself will be a challenge for law enforcement agencies.
4.5.1 Data Security

Victoria Police has no control over the level of security of the social media services it uses. This lack of control puts any law enforcement data potentially at risk.

Facebook, YouTube and Twitter are all used by Victoria Police and have all suffered significant breaches of security.

Facebook has been the subject of numerous external attacks and the exposure of vulnerabilities in its security, placing users’ personal information and their accounts at risk of unauthorised access. A vulnerability that gave advertisers and other third parties a way to access users’ accounts and personal information was uncovered in May 2011\(^\text{128}\). The vulnerability had existed since 2007 and affected close to 100,000 users.

Facebook is also the target of Spam attacks. In 2009 it successfully sued a spammer for obtaining login credentials for user accounts and using those accounts to send spam that linked to phishing sites.\(^\text{129}\) A further Spam attack in 2011 had Facebook users unknowingly copy malicious code into their browser bars that allowed hackers to gain access to their profiles.\(^\text{130}\) The US Federal Trade Commission (FTC) found Twitter to be vulnerable to attack, compromising users’ data, due to Twitter’s use of weak administrative passwords. Two significant breaches of Twitter security in 2009, both cases of unauthorised access to administrative accounts triggered the FTC investigation. Twitter agreed to develop and maintain a comprehensive information security program.\(^\text{131}\)

An online security researcher claimed in 2007 to have uncovered more than 40 security vulnerabilities in Youtube that placed users at risk.\(^\text{132}\) It took some time before Google acknowledged and addressed the issues, claiming to have fixed the vulnerabilities and committing to improving their response to reports of security vulnerabilities.\(^\text{133}\)

Victoria Police need to be aware that the social media services it uses are vulnerable to attack and that Victoria Police can exercise no control over the security of those services. Unauthorised access to a social media service potentially compromises the security of Victoria Police data, members and systems.

4.5.2 Community Expectations

Social media is used principally as a means of communication. Its distinguishing features – interactivity, immediacy and mass-inclusivity – define the expectations of the online community. Law enforcement agencies cannot hope to realign those expectations to fit their own resources or the traditional modus operandi of police. Rather, to use social media effectively as part of contemporary community engagement, police will need to adapt to meet the expectations and protocols of the online community.


\(^{132}\) http://www.theregister.co.uk/2007/06/20/youtube_security_ultimatum/

\(^{133}\) http://www.planetwebsecurity.org/author/Christian_Matthies/
An example from experience that was raised at the roundtable convened by CLEDS was that of response times and accuracy. Response times in the traditional, physical world and those expected on social media are quite different; people expect more immediacy when using social media than they do in their physical-world dealings with police and bureaucracy in general. Police are used to dealing in accurate facts and their response time reflects the degree of accuracy required. It may be, as suggested by one law enforcement agency at the roundtable, that police will need to sacrifice a degree of accuracy in order to meet the expectations of social media users.

4.5.3 Unauthorised Disclosure

Risks relating to unauthorised disclosure are viewed as amongst the most significant in any ‘electronic environment’, as it is very easy to disclose information – in terms of time, quantity and sensitivity – and difficult, if not impossible, to retrieve it. During the drafting of this paper, Victoria Police members raised unauthorised disclosure as a primary risk in relation to the use of social media. Victoria Police’s ‘authorising environment’ specifically addresses the issue of unauthorised disclosure in a number of ways:

- The Police Regulation Act 1958 makes it an offence for a Victoria Police member to disclose any fact or document without authorisation that comes into his or her knowledge by virtue of his or her office. These laws apply to the use and disclosure of personal information on social media sites. Victoria Police’s ethical standards and policy framework also address the issue of unauthorised disclosure.
- The CLEDS Standards address the unauthorised disclosure of law enforcement data as a key information security risk.
- Victorian privacy legislation applies to the collection and handling of personal information, including its use and disclosure (except to the degree that the particular collection, use or disclosure falls within a law enforcement exception).

The possibility of data spills caused by employees posting information not authorised for public release has been cited as the primary security risk for government agencies in relation to social media. CLEDS is aware of Victoria Police breaches of security involving Facebook pages.

It is well known that many social media users fail to consider and apply appropriate privacy settings. As an example, only half of social media website users use privacy settings to control what information they share and with whom, and over a third accept friend requests from people they do not know. However, the unexpected appearance of ‘private information’ with the launch of Facebook’s Timeline and Instagram’s attempts to change its privacy policy mean that more and more individuals are beginning to realise that their personal information is the currency for social media providers and they need to pay attention to privacy.

Victoria Police employees posting information about their personal life, their official duties, project details or government policy could unknowingly provide people with information that could be used to elicit Victoria Police information from them or to tailor social engineering campaigns to compromise the organisation’s networks. Information that appears benign in isolation could, if collated with other information, have a considerable security impact on Victoria Police.

134 Police Regulation Act 1958 (Vic) s 127A.
135 Australian Government Department of Defence, Intelligence and Security Security tips for the use of social media websites November 2012, 1.
136 Ibid, 2.
137 Ibid, 2.
In response, the federal Department of Defence, Intelligence and Security recommends that:

*The use of social media for official purposes should be governed by agency web usage and specific social media usage policies. Enforcing usage policies and implementing mandatory user education on the risks of social media is the key to minimising security risks to government information.*

### 4.5.4 Reputation Management

Social media provides an organisation with an excellent opportunity to improve its public image and reputation, however the nature of social media means that an organisation has less control of its public image than is the case with traditional media. Organisations such as Victoria Police are now required to be more proactive and dynamic in monitoring and responding to threats to their reputation:

*Long gone are the days when media would communicate a brand’s message to consumers. Consumers are now the individuals broadcasting personal or second-hand stories to their social networks and the world. They are a brand’s storytellers and the new brand ambassadors.*

Victoria Police understands that it needs to be proactive in order to minimise any threats to its reputation, *both internally and externally*, as any damage to the reputation of Victoria Police can negatively affect the trust of the public, media relations, and the perceived legitimacy of policing operations.

*Internal risks* are those that originate from within the organisation’s control, such as publications from employees on behalf of the organisation that could be offensive, inappropriate, misleading, and/or dishonest.

*External risks* are viewed as posing the most significant risk to a law enforcement agency’s reputation. External individuals and organisations publishing information about Victoria Police on social media can negatively or positively affect its reputation. Events such as the Occupy Melbourne eviction were heavily discussed on social media services with entries made on Wikipedia and YouTube.

#### Wikipedia and Reputation

Victoria Police does not actively monitor the Wikipedia page on Victoria Police. Members may engage with the page in an unofficial capacity. Users of Wikipedia can look at the edit history of a page and view the revisions, as seen in the image below. They are also able to identify the user profile of those with a Wikipedia account or the IP address of anonymous users.

Recently, the Wikipedia page dealing with Victoria Police contained claims about Police actions during the eviction of *Occupy Melbourne* protestors. Efforts to remove the information have proved futile as other users can reverse any edits. The information posted is publicly available and potentially damaging to Victoria Police’s reputation.

---

138 Ibid, 2.
139 Booth, N. (2011) Mapping and leveraging influencers in social media to shape corporate brand perceptions. Corporate Communications, 16, 3, p. 185
141 [http://www.youtube.com/results?search_query=Occupy+Melbourne&oq=Occupy+Melbourne&gs_l=youtube.3..0l6.144.2307.0.2425.1.5.11.0.4.4.1.189.767.86.11.0...0.0...1ac.1.7yEUm9eCxLg](http://www.youtube.com/results?search_query=Occupy+Melbourne&oq=Occupy+Melbourne&gs_l=youtube.3..0l6.144.2307.0.2425.1.5.11.0.4.4.1.189.767.86.11.0...0.0...1ac.1.7yEUm9eCxLg)
An edit from an obviously frustrated user regarding the Occupy Melbourne claims stated:

*This statement [claims of Police Union and Members actions] is incorrect. The union supports members and has no authority with regard to operational matters. And, to insinuate that Police sexually assaulted protestors in order to remove them is not only incorrect but notably defamatory in its nature. The sexual offences you refer to were made by Occupy persons against other occupy persons. This is the biggest load of crap I have read.*

This post was removed by Wikipedia’s own maintenance systems as seen below, Image 2 (in a message to an anonymous user).

While Wikipedia removed the post, it remains publicly accessible and is attached to IP address 203.25.230.150. This IP address is noted as belonging to ‘Victoria Police Centre, Melbourne, Australia and may be shared by multiple users’.

Clearly, a member (or members) of Victoria Police has been actively engaged in monitoring the Wikipedia page, probably unofficially and without authorisation, using a computer in the Victoria Police Centre.
Additionally, posts that are made to Victoria Police’s social media accounts by external sources can negatively impact its reputation by association. These posts can accuse Victoria Police or its members of corruption and/or be unrelated to the organisation but inappropriate. For example, on the Yarra Ranges Eyewatch page, there have been posts from members of the public accusing police of revenue raising, not serving the public, and grandstanding.

Because social media is less formal than traditional media, its users expect a greater degree of honesty and transparency. Businesses have suffered significant damage to their reputation by being seen as unwilling to communicate openly with consumers via social media. However, the level of transparency that law enforcement agencies can afford is more complex. Law enforcement agencies perform a number of roles that demand a balance between confidentiality and transparency. Community engagement and community policing functions demand a high level of transparency which can be achieved by using a ‘listening and responding’ program, whereas intelligence and criminal investigation call for extremely confidential and non-public action.

4.6 Resourcing

It is commonly stated that one of social media’s key benefits is its ‘cheapness’. However, just as it is clear that privacy can suffer as a result of ‘free’ social media services, so too any genuine engagement with social media is likely to result in a significant financial cost to an organisation. Engaging effectively with social media – i.e. minimising risk and enhancing benefits – may provide Victoria Police with a significant resourcing challenge, particularly if social media is to be integrated as a standard tool across all areas of policing and used to its full advantage.

4.6.1 Staffing

The level of staffing required for effective social media management is dependent on the size and scale of social media presence that is undertaken. As social media is available 24 hours a day, the moderation of social media profiles is likely to be time-consuming and potentially costly. As the number of social media presences expands, this may become a significant issue and no longer feasible financially.

It was noted at the round table convened by CLEDS that the volume of information on social media is already ‘killing’ and that it is physically impossible for law enforcement agencies to carry out monitoring 24/7. Outsourced monitoring or monitoring using software is possible, but costly. Police will need to assess the risks of diminished monitoring, the cost of adequate monitoring and weigh them against the desired outcomes of their social media presence and scale their presence accordingly.

Currently, Victoria Police states that its social media pages are monitored during regular business hours – Monday to Friday from 9am to 5pm. Yet, there is potential for damaging material to be posted or linked to Victoria Police social media pages at any time, including ‘after hours’. As long as a page is available 24 hours a day, 7 days a week, the absence of constant monitoring increases the risk of inappropriate and potentially defamatory material to be posted and viewed by the public.
Users of social media view it as instantaneous and available 24/7. Victoria Police's adherence to ‘business hours’ represents nothing more than an application of a static, old-media paradigm to a new-media order of communication. It looks both old-fashioned (reputation again) and fails to address social media resourcing requirements fully. Further, it should also be noted that monitoring is not a full-time role within Victoria Police, but rather an add-on to other policing functions.

There have been instances where potentially damaging material has remained posted on Victoria Police Facebook pages for over two days (see below, Figure 6, for an example of messages left on the Geelong Eyewatch page for 48 hours).

![Figure 7: Geelong Eyewatch Messages posted by a member of the public](image)

### 4.6.2 Training

In addition to retaining adequate staffing, training those staff is essential to ensure efficient, effective, and secure use of the social media services. By way of example, if social media is to be employed as a daily intelligence tool, with basic intelligence carried out across the operational police force, then intelligence training will be required to a far greater degree than it is now, simply because of the greater quantities of raw data involved. Additionally, greater resources will need to be put into increasing the number of intelligence specialists to handle the inevitable increase in occasions where passive intelligence crosses over to active intelligence, with all the additional costs that this entails.
As Victoria Police broadens its use of social media, more staff will need to be trained in the correct use of social media to ensure efficiency and security. In turn, training Victoria Police members in social media use would require that learning materials be developed and delivered. Because social media is dynamic and ever changing and mutating, training will need to be refreshed periodically and ongoing, requiring considerable financial investment.

4.6.3 Return on Investment

Ultimately, Victoria Police must analyse the risks and effectively plan the resources for the use of social media to ensure that there is an adequate return on any investment in social media. Victoria Police should be very clear about why it is engaging with social media and what it wants to achieve. It should assess its current and potential use of social media and determine the desired balance between its very limited capacity to control the services and the increased capacity they offer Victoria Police to gather intelligence and influence the public through interactivity. Victoria Police then needs to articulate a clear strategy for its engagement with social media.\textsuperscript{142} We do not underestimate the difficulty of this task given the ever changing nature of these media.

A cost-benefit analysis of social media also needs to be undertaken, including a cost-comparison to the pre-social media model. This would enable individuals and organisations to consider the ‘true cost’ of implementing social media and the level of investment required to ensure a suitable return on that investment. For example:

- What is the level of initial and recurrent funding required to ensure that social media is able to operate effectively, efficiently and meaningfully across the whole of Victoria Police?
- Is there any potential for social media to become as costly as the large-scale ICT projects that have come before it?
- Knowing now what we do about over-budget and under-performing ICT initiatives, are there useful lessons to apply to social media implementations?

4.7 Governance and Policy

Little thought had been given until recently to developing and implementing an adequate governance structure to regulate the use of social media by Victoria Police, or other Australian police jurisdictions. The approach has been unsystematic and siloed. While this reflects the discrete uses by police of social media and disparities in the rate of development of those uses, there is a need for a centralised governance structure that acknowledges the considerable overlaps between the various uses of social media – community engagement, for example, is about more than communications and reputation, but a valid source of intelligence, and any use of social media where police identify as police brings with it issues of reputation.

\textsuperscript{142} The Victorian Department of Health Social Media Action Plan Pt. 2: Staff Toolkit provides a useful example of how to ensure that any social media use meets its specified goals. In particular, it suggests that public sector organisations:

- Establish clear and transparent measures for social media implementations
- Regularly evaluate the success of social media tools and applications
- Select and structure measures to match the objectives of the site and of the brand.
Victoria Police has now acknowledged the need for a central body to oversee and steer the direction of its social media policy and strategy, taking into account the different uses for social media within law enforcement. It has established a Social Media Steering Committee. The Committee brings together senior officers in charge of the Crime, State Emergencies and Security, Intelligence and Covert Support Commands, the Directors of Information Management, Security and Standards, Legal Services and IT Services and a regional Assistant Commissioner representing frontline policing.

The Social Media Working Group will, among other things:

- set the strategic direction for the introduction and management of social media throughout Victoria Police
- make recommendations on priorities and issues
- oversee the development and direction of a social media strategy and its timely implementation
- establish a workable governance model for the management of social media issues
- manage and, where possible, identify risks related to social media and oversee strategies to mitigate those risks
- drive collaboration within the organisation and with key stakeholders
- monitor organisational effort and spend on social media related projects/activities and ensure they meet organisational priorities
- establish a measurement framework for the delivery of social media projects
- drive cultural change on information management related issues.

It has been common for Australian law enforcement agencies to place primary responsibility for social media within their communications and media departments. However, if police are to effectively use social media as a tool of operational policing, responsibility should properly sit within an operational department, certainly in close cooperation with media and communications.

The evaluation report of the Facebook pilot recommends that if the pilot is to continue, it be transferred to an operational policing responsibility and managed via the Intelligence and Covert Command. The report notes that ‘(t)he benefit of having an operational department take carriage of the project is their ability to further work with the members to explore operational possibilities of using Facebook as a policing tool, whilst maintaining appropriate police procedure.\textsuperscript{143}

The establishment of a broad-based, but principally operational Social Media Steering Committee is evidence that Victoria Police is fully aware of where responsibility for social media properly sits if it is to be used a standard law enforcement tool.

While Australian police jurisdictions have generally introduced social media policies, they are not mature documents. The policy context within which law enforcement agencies are able to manage and use social media is emerging and is far from settled. Most law enforcement agencies represented at the CLEDS roundtable indicated that due to the complexity of the operating environment and the dynamic and ever changing nature of social media, it is at this stage difficult to establish clear guidelines and frameworks within which to oversee their operations.

\textsuperscript{143} Operational Use of Facebook (Pilot) Evaluation Report, Victoria Police April 2013.
It was recognised at the CLEDS roundtable that there needs to be a coherent national policy and legal framework within which law enforcement and justice can operate with regard to social media. Coordination at a national level is required as social media doesn’t recognise jurisdictional boundaries.

4.8 Final Comments

The use of social media for policing purposes raises a broad spectrum of benefits, issues and risks. It is highly likely that Victoria Police will need to consider some of these issues and risks in greater detail before making any decisions if, how and to what extent to expand its use of social media. So too, there are other issues that have not been assessed in this report, including ‘take down’ requests, the admissibility of social media evidence and human rights. There is, for example, a need to clarify how best to balance that which is in the public interest with the rights of the individual. This is a key question that needs to be explored in terms of law enforcement and operational policy.144

The report indicates that the general anxiety about whether or not current laws apply to social media appears to be misplaced; on the other hand, this may not provide comfort when jurisdictional issues are taken into account. Nevertheless, publicising the way in which offline laws apply to social media may help to facilitate a shared understanding of the need for social media (and its users) to comply with a range of offline requirements. Where this is unclear, existing laws may need to be clarified and/or extended for example, ensuring social media is covered in the same way as email or SMS under telecommunications provisions.

The prospect of social media – in particular, Facebook – providing a firm basis for operational policing appears fraught, not least because of the application of the CLEDS Standards. Further, Facebook’s launch of its ‘in-house’ search engine, Facebook graph, in addition to its private messaging service (email), suggests metaphors of Facebook as a ‘walled garden’ may well soon change to a ‘fortress city’ from which member never (need to) leave. If Facebook ‘becomes a central platform – a closed silo of content, and one that does not give you full control over your information in it’, it is no appropriate place to leave Victorian law enforcement data.

144 For example the right of the community to know versus the right of an individual to be treated fairly before the law can be challenging with the existence of social media.
This page is intentionally left blank.