

Can I Follow You? Social Media Surveillance and Policing Dilemmas

by

Liam Cahill

Canterbury Christ Church University

**Thesis submitted
for the MSc by Research**

2020

Abstract

This research paper explores current open source practices within the Metropolitan Police Service (MPS), with specific attention to social media use by frontline personnel for the purpose of intelligence gathering, investigation and safeguarding. Although, still a relatively new phenomenon for policing, recent advancements have been made in understanding the impact of open source and social media data use in police work, but the focus has been limited to overarching thematic analysis of systems that suggest institutional coordination in their use, function and purpose. This study takes a different approach by focusing on the practices employed by frontline policing personnel in the Metropolitan Police Service and evaluates the concept of ‘localised surveillance’ practices employed by frontline officers that risk undermining police legitimacy at a fundamental level. By identifying localised practices that include the use of personal devices, personal social media accounts and false personas to covertly extract open source and social media data this research considers the shifting power relationship between the police and public in an age where a plethora of personal information is readily available on the internet. At time when traditional surveillance practices are the focus of public enquiry, this timely and relevant research is essential for police services’ nationally and beyond to consider the implications of localised surveillance practices by frontline personnel on their respective agencies and society more widely.

Keywords – social media, surveillance, Metropolitan Police Service, open source, intelligence, investigation, safeguarding, policing, localised social media surveillance.

Acknowledgements

This research thesis has been two (2) and half years in the making and there are people that absolutely deserve to be acknowledged and thanked for their support. First and foremost is my wife Fayruz. Having been together for 12 years she has tirelessly supported me, not only throughout the master's degree and has been there for me every step of the way. In 2018 she gave me the greatest gift I could ever wish for with the birth of my son Aidan. His arrival had been a long journey filled with many disappointments and challenges but Fayruz stayed strong and was a constant source of inspiration for me to do the same. Fayruz, you are my world, thank you! x

I would like to thank Dr Emma Williams and Dr Steve Tong from Canterbury Christchurch University you have both been incredibly supportive over the years and it has been a pleasure experiencing this academic journey with you both. Emma on a personal note, thank you for your continued guidance and support over the years, your tutorship has made this journey a pleasure to be a part of. Thank you!

I would like to thank both the Metropolitan Police Service and the College of Policing for authorising this research, supporting it through the bursary scheme in 2017/2018 and for supporting me with academic leave in order to progress the research. It was always a consideration from the beginning that the results would be controversial but would provide an opportunity to evaluate current practice and strive to improve with a clear understanding of what needed to be achieved. Organisationally it was brave to allow this research to be embarked upon and for that and the opportunity to develop I thank you.

Finally, a message to my son, Aidan. You are only seven months old at the time of writing and you're already the most amazing person I know. I am so sorry for the time that I have spent away from you in order to complete this research. I hope one day when you are studying for a test, researching for a paper, preparing for a job interview or completing

your PhD and when everything seems tough, you'll look back on this message to help drive you across the finish line. Throughout my life there have been more people put me down and try to stop me achieving than I care to remember, including friends and family who mocked me at an early age for my difficulty in reading, writing and spelling. Many told me, 'You can't', 'You won't be able to', 'That won't happen' and the completion of this masters degree is no exception. Yet today I submit this thesis, completed and dedicated to you. Throughout your life you may encounter similar attitudes, I hope you don't but if you do, I want you to remember both your mum and I believe in you and there is nothing you can't do with determination and hard work, don't let anyone stop you from achieving your full potential and dreams. All my love, dad x

Contents Page

Contents	Page No.
<u>Title Page.</u>	<u>1</u>
<u>Abstract.</u>	<u>2</u>
<u>Acknowledgements</u>	<u>3</u>
<u>Contents Page</u>	<u>5</u>
<u>List of Tables and Figures</u>	<u>8</u>
<u>Chapter 1. Introduction and Research Aims</u>	<u>12</u>
<u>Chapter 2. Literature Review</u>	
<u>2.1. Surveillance and Social Control</u>	<u>17</u>
<u>2.1.1 Police Surveillance</u>	<u>19</u>
<u>2.1.2 Policing Legitimacy and Power</u>	<u>21</u>
<u>2.1.3 Legislation, Policy and Ethics</u>	<u>23</u>
<u>2.2. Social Media in Policing</u>	<u>28</u>
<u>2.2.1 Social Media for Engagement</u>	<u>29</u>
<u>2.2.2 Social Media for Intelligence and Investigation</u>	<u>31</u>
<u>2.2.3 Social Media Surveillance</u>	<u>33</u>
<u>Chapter 3. Methodology</u>	
<u>3.1. Introduction</u>	<u>36</u>
<u>3.2. Police Research</u>	<u>36</u>
<u>3.3. Philosophical Perspective</u>	<u>38</u>
<u>3.4. Research Design</u>	<u>41</u>

<u>3.4.1. Research Method</u>	<u>41</u>
<u>3.4.2. Reliability and Validity</u>	<u>43</u>
<u>3.4.3. Phase One – Focus Groups</u>	<u>45</u>
<u>3.4.4. Phase Two – Survey</u>	<u>50</u>
<u>3.4.5. Ethical Considerations</u>	<u>58</u>
<u>3.4.6. Personal Reflections</u>	<u>60</u>

Chapter 4. Results and Discussion

<u>4.1. Introduction</u>	<u>64</u>
<u>4.2. Open Source and the Front Line</u>	<u>67</u>
<u>4.2.1. Frequency of Open Source Use</u>	<u>74</u>
<u>4.2.2. Personal Social Media Accounts</u>	<u>76</u>
<u>4.2.3. False Personas</u>	<u>79</u>
<u>4.2.4. Personal Devices</u>	<u>83</u>
<u>4.3. Open Source in a Policing Context</u>	<u>87</u>
<u>4.3.1. Safeguarding V’s Investigation/Intelligence</u>	<u>88</u>
<u>4.3.2. Personal Device Use</u>	<u>92</u>
<u>4.3.3. Why Personnel don’t use i3 (Open Source) Team</u>	<u>97</u>
<u>4.3.3.1. Efficiency</u>	<u>99</u>
<u>4.3.3.2. Restrictive IT Systems</u>	<u>101</u>
<u>4.3.3.3. Its Open Source</u>	<u>102</u>
<u>4.3.3.4. Self Service</u>	<u>102</u>

<u>4.4. Policing Dilemmas and Open Source</u>	<u>105</u>
<u>4.4.1. Legislation: Regulation of Investigatory Powers Act 2000</u>	<u>105</u>
<u>4.4.2. MPS Policy</u>	<u>108</u>
<u>4.4.3. College of Poling Code of Ethics</u>	<u>110</u>
<u>4.4.4. Policing Attitudes towards Privacy/Security</u>	<u>111</u>
<u>Chapter 5. Summary, Recommendations and Concluding Remarks</u>	
<u>5.1. Summary</u>	<u>116</u>
<u>5.2. Recommendations</u>	<u>121</u>
<u>5.2. Concluding Remarks</u>	<u>124</u>
<u>References</u>	<u>126</u>
<u>Bibliography</u>	<u>139</u>
<u>Appendices</u>	<u>143</u>

List of Tables

Table No.	Title	Page No.
Table 1	Level of training in internet investigation and research.	174
Table 2	Methods of training received.	175
Table 3	Access to an MPS social media account.	176
Table 4	How often do you use online investigation in your work?	177
Table 5	Awareness of the open source unit.	180
Table 6	How have you conducted online research?	181
Table 7	Reason for using your personal device for online research.	182
Table 8	Reasons why the Open Source Unit (OSU) were not used.	186
Table 9	Use of personal social media for online investigation and research.	188
Table 10	Use of a false persona for online investigation and research	190
Table 11	Frequency of False Persona use at each Open Source Level	190
Table 12	What devices have you used when using a false persona	191
Table 13	What your current rank/grade is?	192
Table 14	State your length of service.	193
Table 15	select your age group.	194
Table 16	Does RIPA Impacts obtaining OS Intelligence	195
Table 17	Does MPS Policy obtaining OS Intelligence?	197
Table 18	Does the Code of Ethics apply to the use of Open Source?	198
Table 19	Automatic right to view OSINT regardless how personal?	199

<u>Table 20</u>	<u>Level 1 Frequency of Open Source Investigation by Grade/Rank.</u>	<u>75</u>
<u>Table 21</u>	<u>Use of Personal Social Media Account across Age/Service/Rank.</u>	<u>78</u>
<u>Table 22</u>	<u>Level 1 use of a False Persona across Age/ Service/Rank.</u>	<u>82</u>
<u>Table 23</u>	<u>Use of personal device to conduct online investigation research across</u>	
	<u>Open Source Training/Age/Service/Rank Demographics.</u>	<u>85</u>
<u>Table 24</u>	<u>Ch. 4.2 Summary of key findings and inferences against MPS Population.</u>	<u>87</u>
<u>Table 25</u>	<u>Word frequency for question 5. Briefly describe how you use/have used</u>	
	<u>Online Investigation.</u>	<u>89</u>
<u>Table 26</u>	<u>Ch. 4.3 Summary of key findings and inferences against MPS Population.</u>	<u>104</u>
<u>Table 27</u>	<u>Ch. 4.4 Summary of key findings and inferences against MPS Population.</u>	<u>115</u>
<u>Table 28</u>	<u>Summary of all Estimated Population Proportions across research areas.</u>	<u>116</u>

List of Figures

Table No.	Title	Page No.
Figure 1	National Internet Investigation Model.	27
Figure 2	List of questions for thematic coding strategy.	50
Figure 4	Focus Group Coding Analysis.	168
Figure 5	Respondent's level of open source training (Pie chart)	174
Figure 6	Have you received social media training? (Pie chart)	175
Figure 7	Access to an MPS social media account. (Pie chart)	176
Figure 8	How often do you use online investigation (Open Source)? (Pie chart)	177
Figure 9	Qualitative Comments and Thematic Coding: Question 5.	178
Figure 10	Awareness of the i3 (open source) Team. (Pie chart)	180
Figure 11	How have you conducted online research? (Horizontal bar chart)	84
Figure 12	Reasons for using your personal device (Bar chart)	95
Figure 13	Qualitative Comments and Thematic Coding: Question 7.1.	183
Figure 14	Reasons why i3 (open source) Team not used (Horizontal bar chart)	186
Figure 15	Qualitative Comments & Thematic Coding (Other Comments): Q.8.	187
Figure 16	Have you ever used your personal social media account. (pie chart)	76
Figure 17	Qualitative Comments and Thematic Coding: Question 9.	188
Figure 18	Have you ever used a false persona. (Pie chart)	81
Figure 19	What devices have you used a false persona on? (Pie chart)	191
Figure 20	What is your current rank/grade? (Pie chart)	192
Figure 21	What is your length of service? (Pie chart)	193

Figure 22	State your age range. (Pie chart)	194
Figure 23	Does RIPA Impacts obtaining OS Intelligence. (Pie chart)	195
Figure 24	Qualitative Comments and Thematic Coding: Knowledge Q.1.	196
Figure 25	Does MPS Policy obtaining OS Intelligence? (Pie chart)	197
Figure 26	Does the Code of Ethics apply to the use of Open Source?	198
Figure 27	Automatic police right to view OSINT regardless how personal?	199
Figure 28	Qualitative Comments and Thematic Coding: Knowledge Q.4.	200
Figure 29	Level 1 trained personnel use online investigation. (Word Cloud)	92
Figure 31.	Comparison between concepts of State Surveillance and Local Social Media Surveillance.	120

Chapter 1. Introduction and Research Aims

As society increases its consumption of mobile technology with round the clock access to social media platforms that require user generated content to survive; from commonplace breakfast selfies to drill videos validating gang affiliation. Law enforcement continues to recognise the value of open source and social media as an important tool to prevent crime, collect evidence and assist in identifying individuals associated with criminal activity (LexisNexis, 2014, p.9). With increased user driven content comes the exposure of personal data providing others the ability to observe, watch, surveil. Law enforcement survive on the identification and extraction of intelligence to prevent crime and disorder and their appetite to harness publicly available intelligence is only growing in tandem with technological advancements. It is well documented that law enforcement agencies around the world are investing heavily to harness the power and opportunities of open source technology but the focus of research remains largely limited to ‘outsider’ analysis of open source and social media as a law enforcement tactic and generally focuses on the concept of surveillance at the institutional level or above.

This research has considered the current literature on the use of surveillance as a social control measure and the adaptation of surveillance power since Foucault reflected on the ‘observation of the many by the few’(Mathiesen, 1997, p.216). With advancements in communications technology, social media has changed our understanding of the power dynamics involved in surveillance and evolved traditional hierarchical surveillance models to include multi-directional and lateral surveillance behaviours. Surveillance is considered here in a policing context and reflects on the consequences of unchecked surveillance by policing personnel. An issue which has drawn significant attention in recent years through the inquiry into undercover policing practices and although it focuses primarily on traditional tactics it recognises the transition of covert practices from

physical to digital (Mitting, 2015, p.3). The adoption of new surveillance practices impacts the notion of policing legitimacy especially as these new technologies provide greater insights into individuals private lives that require a need for balance across the conflicting paradigms of security and privacy. In some respects, social media offers less intrusive access to intelligence compared to traditional tactics; nonetheless embracing these open source opportunities rightly places responsibility for proportionality and necessity at the feet of law enforcement as power holders in their pursuit of effective intelligence gathering.

The governance of social media surveillance is considered here in terms of legislation, primarily under the *Regulation of Investigatory Powers Act 2000*, current policy and ethics. In addition, room to explore the legitimate use of social media as a tool for engagement, intelligence and investigation in policing has been provided in order to acknowledge the role these combined elements play in establishing a culture of accepted social media surveillance practices within policing. This is highlighted through the recognition that the key legislation is considered unfit for purpose leaving a vacuum for interpretation to flourish.

This study recognises that little attention is given to the open source activities of policing personnel, who can access the same mobile devices and social media platforms as the public and possess the capability to conduct open source research at the swipe of a phone screen. A lack of internal organisational access has resulted in researchers concentrating on the impact of organisational scale surveillance, with academia overlooking the concept and impact of 'localised social media surveillance' practices by the police on society.

The combined research arena of open source, social media and their impact on Law Enforcement creates a substantial field in which to work and it is necessary to ensure this research has concise aims to remain focused. Therefore, the aims of this study are;

- To establish what the current social media practices being employed by policing personnel across the MPS and determine whether they constitute a form of surveillance.
- To establish whether any identified practices highlight gaps in current policy.
- Deliver a new theoretical interpretation of surveillance in the context of social media and policing.

This research provides value in understanding of current policing tactics in relation to the use of open source and social media and considers their use in a surveillance context. The State is represented by the activities of the police and the public are entitled in a democratic society to have trust in the fair application of the law. The police must therefore balance the proportionate needs of conducting surveillance for the purposes of security with the human right to individual privacy.

The results and discussion have been divided into three overarching themes to assist in exploring the aims listed above. They are '*Social Media and the Front Line*' which will evidence the demographics using the open source for intelligence and investigation purposes and the frequency of its use. The second theme '*Social Media in a Policing Context*' will consider what MPS personnel use open source and social media in a policing context for and why and finally the third theme is '*Policing Dilemmas and Social Media*' exploring the implications of these behaviours. However, the focus of this research will centre on the MPS personnel's reliance of their own mobile devices, personal social media accounts and false personas for intelligence gathering and investigations. This will demonstrate that practices have established themselves as

‘normative culture’ where the distinction between public and private digital spaces has been blurred by practitioners who rationalise and justify access to publicly available information under the banner of ‘policing purpose’ and consider the internet ‘fair game.’ By considering the frequency of these practices and their impact on the legitimacy of policing this research will argue that these practices have penetrated the cognisance of MPS personnel at all levels of frontline policing. Fundamentally this will raise procedural, legislative and ethical questions around the use of social media surveillance activities, the role of policing in these digital spheres, MPS personnel’s understanding of privacy and the impact these practices have on concepts of police legitimacy and the power relationship between the police and the public. These are not just issues for the MPS but issues important to National Policing as the concepts identified here will have implications for all police services across the United Kingdom.

Combining positivist and interpretivist methodological approaches in a mixed method design, this study obtained qualitative data from focus groups and quantitative and qualitative data from an MPS wide survey. This triangulated analysis represents the first internal study of operational practices by officers and staff and provides an insight into unchecked frontline social media surveillance. The scale of the practices concludes systemic challenges resulting from inadequate access and control over the use of open source intelligence for and by personnel. While the findings raise concerns over policing practices locally, they also represent a significant challenge for the management of covert online surveillance for policing nationally, if not globally. As an ‘insider-insider’ this paper provides a unique operational insight not previously captured, with the closest study performed by LexisNexis (2014) that looked at US Law Enforcement and the frequency of social media use across a range of policing duties. While previous research considers the implications of social media surveillance at an organisational level, usually referencing social media monitoring (Williams, *et al*, 2013, pp.461-481; Fuchs and

Trottier, 2015, pp.113-135; Sampson, 2017, pp.55-69; Trottier, 2015, pp.317-333). This original study considers social media surveillance practices by individuals at the local level and the implications their combined activities have on policing legitimacy. In evaluating the findings this research concludes by proposing a number of recommendations to the current approaches of acquiring open source intelligence and suggests a new theoretical interpretation to articulate the practices observed, namely, 'Localised Social Media Surveillance' (also referred to as 'Localised Surveillance' in this research). The concept of 'Localised Surveillance' denotes the use of open source, specifically social media on a local level by power holders (the police) for a localised purpose, examples of which include the use of social media surveillance in localised criminal investigations, searching for a missing person and gathering local intelligence on a local known audience.

In identifying and defining the phenomenon of 'localised social media surveillance' this research has supported the creation and implementation of practical solutions to minimise its occurrence. The MPS is currently seeking to deploy an alternative approach to the acquisition of open source and social media data that is fully auditable and transparent, while increasing availability of access to frontline personnel. Combined with targeted training and intervention based on the demographic results of this study there is an opportunity to reduce the current practices significantly ensuring the protection of MPS personnel from disciplinary action or unnecessarily exposing of their own personal data to those involved in criminality. Additionally, the recommendations within this research seek to protect the organisational reputation while increasing the public's confidence in the use of social media technologies by police services. The results also act as a guide to other police services across the country who may also be experiencing the effects of localised social media surveillance.

Chapter 2. Literature Review

2.1. Surveillance and Social Control

The observation of others to obtain information has always been a feature of human nature, with one of the earliest examples of surveillance coming from the Book of Genesis. In this biblical writing, God's one rule to Adam and Eve in the Garden of Eden is disobeyed yet clearly observed (Lyon, 2003b, p.1). Surveillance according to Fuchs (2011, p.124) is a control mechanism to, 'oversee' or 'watch over' and is carried out by 'watchers', 'overseers' or 'officials' signifying a hierarchical power dynamic between those watching and those being watched. While Lyon (2001, p.2; 2003b, p.5) arguably provides a more accurate reflection of modern society defining surveillance as, 'the routine collection and processing of personal data, whether identifiable or not, for influencing, managing or controlling certain persons or population groups.' This fits more accurately with societies ability to watch and collect data about each other where Fuchs hierarchical definition fails to consider 'self-surveillance' (Surette, 2016) also known as 'lateral surveillance' (Ball, Haggerty and Lyon, 2012, p.344) or 'interveillance' (Fuchs *et al*, 2012, p.231) through one's peers or 'power' equals. On the one hand this has been considered as a positive aspect to surveillance which empowers users to see surveillance as social and involves participatory acts of mutuality and sharing (Albrechtslund cited in Fuchs *et al*, 2012, p.128) and in this new era of digital 'self-surveillance', online communities can self-regulate, challenge and report inappropriate behaviour (Press Association, 2012) through a process of this 'participatory surveillance' (Trottier and Lyon cited in Fuchs *et al*, 2012, p.91). On the other hand, Fuchs *et al* (2012, p.127- 129) agrees with Kose, Han and Bakan who articulate that it is the act of watching each other [through social media] that is an ideal architectural example of modern disciplinary power that gradually creates a social pressure in the context of creating a homogenous attitude that discipline and control normalise peoples' behaviours.

Foucault (Faubion, 2002, p.58-59) discusses these ideas as he elaborates on Bentham's original panopticon design for prisons, which allowed the 'few' in authority to monitor the 'many' without power from a central position; with its success resting not simply in the architectural design but in the psychological domination of the powerless 'watched'. Perceiving their actions to be under constant observation the imprisoned were obedient out of fear of being seen (Fuchs *et al*, 2012, p.127). However, Kose, Han and Bakan (2010, p.254) studied the power dynamic in surveillance and suggested a 'power reversal' in modern times where people such as politicians and celebrities are now monitored by the masses, altering Bentham's original viewpoint to argue the 'many now monitor the few.' Lyon (1998, p.94) questioned the application of Foucault's work to electronic surveillance and while a different paradigm, parallels can be drawn from the widespread implementation of CCTV as a social control mechanism. It was installed to foster the perception in society that actions were under constant observation with the intention of deterring crime and ensuring civil obedience (College of Policing, 2013, p.1). However, Walsh and Farrington (2007, p.7) argued that the presence of CCTV is only effective to a limited degree or when targeting specific crimes (College of Policing, 2013, p.1) supporting Gottfredson and Hirschi's (1990, p.270) view that there is no evidence to suggest that an escalation of surveillance generally influences crime levels.

This is important as police services begin to see social media with panopticon value, (Fuchs *et al*, 2012, p.127) where they can monitor the 'many', but in stark contrast to Bentham's moral architectural (Lyon, 1991, p.597) approach to prisons, social media surveillance offers law enforcement more than just a visual audit of one's actions or potentially their 'actus reus' (guilty act) as users document their thoughts, beliefs and intimacies publicly they also expose their potential 'mens rea' (guilty mind) too (Surette, 2016). McMullen (2015) goes on to consider the 'relative intangibility that data

surveillance offers where there is no physical sense of exposure to authority as the difference between Bentham's panopticon design.' Stating, 'without an explicit sense of exposure actions are not normalised, if anything the supposed anonymity of the internet means users do the opposite,' and act without fear of the repercussions. This has created significant challenges for law enforcement who have recognised the need to have a covert surveillance presence within the digital space (ACPO, 2013, p.10).

2.1.1. Police Surveillance

Traditionally police surveillance has been concerned with direct observation (Lyon, 2003b, p.6) fostering images of targets being followed and observed in close quarters. Press Association (2015) recognised that 'only five years ago a suspect physically walked into a bank and carried out transactions, we could put a surveillance team on that but now, it's mostly online.' While there is still a place for these covert tactics, they have given way to an increased use of digital surveillance and the internet (ACPO, 2013, p.5). Which has enabled law enforcement to exploit social media platforms for intelligence that provides access to individuals and groups whom previously would have required more intense, covert tactics to obtain actionable information (Procter, 2013, p.420). The 2018 guidelines on covert policing (Great Britain. Home Office, 2018, p.18) consider the use of open source surveillance as a less intrusive tactic compared to traditional methods of physical covert surveillance. This is because open source research does not generally interfere with individuals right to privacy under article 8 of the *Human Rights Act 1998*, and in most situations no authorisation is required under the *Regulation of Investigatory Powers Act 2000* as the information is readily available in the public domain.

The focus on police surveillance in the UK have never been more prominent with media reports exposing sexual relationships between undercover officers and those being surveilled (Evans, 2018). Revelations that prompted the Metropolitan Police Service

(MPS) to initiate an internal review of their covert practices in 2011 (Evans, 2018b) and lead to the start of a formal inquiry into undercover operations reaching back to 1968. The inquiry launched in 2015 will primarily focus on physical undercover activities but its scope will include the growing need to conduct covert activities online (Mitting, 2015, p.3). With such emphasis placed upon traditional covert practices there is a gap in the literature around what covert practices are taking place on social media by law enforcement.

While social media is a relatively new technology that can be harnessed to the benefit of law enforcement it is not the first instance of technology being adopted to tackle crime. In almost Orwellian fashion, ‘the UK delivered an extensive CCTV programme between 1999 – 2001’ (Welsh and Farrington, 2007, p.11) and similarly its use was met with privacy concerns when it was adopted as a way of reducing crime and improving security (Wacks, 2015, p.3). A 2007 report estimated that there are 4.2 million CCTV cameras (Bell, Haggerty and Lyon, 2012, p.142) in Britain or 1 for every 14 citizens, recording individuals approximately 300 times each day (Welsh and Farrington, 2007, p.7). While the scale of CCTV use raised concerns, the 2001 terrorist attack on the World Trade Centre provided a catalyst for a ‘resurgence in the value and use of criminal intelligence’ (ROSA, 2017, p.3) and was suggested by Lyon (2003b, p.4) as the ‘golden opportunity’ to implement more robust surveillance initiatives under the banner of the ‘War on Terror’ (Lyon, 2003b, p.15; Ball, Haggerty and Lyon, p.169) creating a ripple effect that would impact citizens globally. Subsequent terrorist attacks in the UK reinforced a social movement encouraged by law enforcement for citizens to become the eyes and ears of unknown future attacks, establishing an environment that normalised suspicion among community members and a galvanised a willingness to sacrifice liberties over security based on the heightened emotional response to these events (Lyon, 2003b, p.56). This cultural shift fostered the perception that if you have nothing to hide, then you have

nothing to fear and increases law enforcement's legitimacy to exercise more intrusive power over citizens information. However, Solove (2011, p.21-23) details by accepting in this position individuals fail to safeguard a position that although they have nothing to hide, equally they may have nothing they wish to share.

2.1.2. Policing Legitimacy and Power

According to Homolova (2018, p.93) institutions are closer to citizens than ever, with former strict hierarchies of power giving way to democracy which places a high demand on [policing] legitimacy needing to justify the necessity of power in their maintenance of order. Bottoms and Tankebe (2012, p.124) consider the 'right to rule' from the standpoint on both citizens and power-holders believing the key question to ask is, 'whether a power-holder is justified in claiming the right to hold power over other citizens?' With 8 in 10 law enforcement professionals actively using social media as an investigation tool (LexisNexis, 2014, p.2) this is an important question as police officers are increasingly compelled to carry out research and investigations using the internet (MPS, 2014c, p.12). Ultimately spending more time collecting and processing personal [digital] information (Ball, Haggerty and Lyon, 2012, p.2) that can generate voluminous records of [citizens] activities (Brown, 2015, p.2).

According to Bottoms and Tankebe (2012, p.121) police legitimacy is present when, 'citizens are treated fairly in decisions affecting them and that they are treated with respect during the process, which ultimately determines whether the decision is accepted.' This definition challenges police legitimacy in the application of social media surveillance as citizens are unaware that they are under any form of observation or that their data is being used in decisions that will affect them. Consequently, their lack of awareness prohibits citizens the ability to ensure that their data is being used with respect and raises questions around historical concepts of 'policing by consent' (Great Britain. HMIC, 2014, p.73).

However, as criminal trends develop and embrace new technologies it is essential law enforcement agencies have access, presence and capability to ensure public safety as considered by the Mayor of Police and Crime (MOPAC) in London Assembly (2013, p.33). The increased corporate use of social media as a communication tool in policing has legitimatised its use by officers (College of Policing, 2017), yet while the corporate mandate is predominantly aimed at community engagement, there is potential for untrained officers to use social media for observation purposes, creating unchecked surveillance creep amongst the front line. This is an issue considered by Cameron (2016) who quotes Jay Stanley from American Civil Liberty Union who states, ‘Even though you obviously don’t need a warrant to read stuff that’s been published for the world to see, that doesn’t mean as a policy matter it’s a good idea for us to give our police licence to engage in mass social media monitoring.’

The legitimacy of police intelligence gathering raises academic friction between the fear of increased security v’s the impact on individual privacy with Trottier (2015a, p.537) suggesting there is no issue with law enforcement using of open source data, as this is publicly available. Which conflicts with Bartlett *et al* (2013, p.22) who states, ‘just because information is open source, does not necessarily mean the police should collect or analyse it’ and the standards of proportionality and necessity should still apply to open source acquisition. Ultimately it is the responsibility of government and law enforcement agencies to balance public safety with protecting the privacy rights of the innocent engaging in lawful activities using those same technologies (London Assembly, 2013, p.32; Press Association, 2015).

According to Bottoms and Tankebe (2012, p. 120) ‘legitimacy is dialogic between power holders (e.g. government/police) and audiences’ (e.g. the public). Legitimate authorities must not only have the power but also the right to govern and audiences must recognise

that right.’ To foster public support and garner legitimacy some law enforcement agencies have resorted to relabelling similar technologies by creating a distinction between social media monitoring and social media alert systems. In a Boston Radio interview O’keefe and Chakrabarti (2016) discusses the distinction between the Arlington Police Department who received praise for the use of ‘Social Sentinel’ an alert system based on key word scraping of open source media against the Boston Police Department who were publicly criticised for their discreet implementation of a monitoring program and maintaining covert online profiles. As Bekker, Edwards, Kool (2013, p.335) conclude, social media monitoring creates tensions, it can work in the publics favour driving causes and bringing attention to important issues. While on the other hand, social media monitoring involves ordinary citizen’s communications in virtual domains that they may perceive as private. This poses ethical questions, especially when the monitoring agency is not transparent regarding its monitoring activity. It is for this reason that an appropriate combination of legislation, policy and ethics has to be employed to ensure the correct balance of power and legitimacy.

2.1.3. Legislation, Policy and Ethics

Bartlett *et al* (2013, p.22) recognises for law enforcement to use Social Media Intelligence (SOCMINT) with confidence, attention must be given to the legislation, ethics and regulations governing its handling. Clapham (2015, p.110) goes on to consider public perception and approval, stating if the police use such surveillance tactics, they need to be transparent, proportionate, necessary and used only to achieve a legitimate aim. However, navigating these challenges during routine policing duties can be daunting for the average beat officer, consequently UK law enforcement, including the Metropolitan Police have established Local Intelligence Teams (LITs) in addition to central Internet

Investigation and Intelligence (III) unit who specialise in open source investigations to support officers traversing this complex area (Bartlett, 2015, p.8; MPS, 2014b, p.8).

A range of legislation is considered when looking at the use of social media for community engagement as highlighted in MPS (2015b, p.2; 2014, p.6), however the key legislation concerning surveillance is contained within the *Regulation of Investigatory Powers Act 2000* and is impacted by Article 8 of the *Human Rights Act 1998*. The *Regulation of Investigatory Powers Act 2000* covers the interception of communications, intrusive surveillance, directed surveillance, covert human intelligence sources and communications data.

The key components of surveillance that render a legal authority necessary under the *Regulation of Investigatory Powers Act 2000* are that activity must be covert, intrusive or capable of obtaining private information about a person. Creating a conflict with the nature of open source surveillance which is publicly accessible and can be obtained overtly. Charles Farr cited in Bowcott and Ball (2014) points out ‘the *Regulation of Investigatory Powers Act* was created before social media existed’ and so pays no reference to social media or the legal boundaries of open source surveillance. As many social media companies have international bases they fall under the definition of ‘external’ communications. This has led to practitioners having no clear legal direction on what is acceptable in terms of conducting social media surveillance investigations (Bartlett, 2013, p.9), with Bowcott and Ball (2014) documenting calls for the *Regulation of Investigatory Powers Act 2000* to be urgently overhauled.

Such concerns led to the proposed implementation of the *Investigatory Powers Act 2016* also known as the ‘snoopers’ charter’ (BBC, 2015) which compels communications firms to hold user’s previous communications metadata for a year, which includes the who, when, where and for how long the user was connected to the internet (Cobbe, 2018, p.10).

According to the BBC (2015) this new information includes details of services, websites and data sources users connect to and is called a user's 'Internet Connection Record' (ICR). Under existing legislation authorities can ask for this data going forward but not retrospectively, this change has caught the concern of Liberty (2016, p.14) who state that this effectively modifies the presumption of innocence and brings all citizens under suspicion, as all digital actions are recorded.

However, since the proposed legislation came to light Liberty have been challenging its compatibility with Articles 8 of the *Human Rights Act 1998*. In 2015 the European Court of Justice agreed that as data collection under *Investigatory Powers Act 2016* was indiscriminate, rather than targeted, it was unlawful (Evans, 2018a). A further Court of Appeal ruling confirmed that the *Investigatory Powers Act 2016* did not restrict the accessing of personal data to investigations of 'serious crime' and allowed police and other public bodies to self-authorise surveillance without adequate oversight (Travis, 2018). Similar concerns were raised in Office of Surveillance Commissioners report cited in Hill (2017) where it became apparent local authorities were regularly using social media in investigations for a wide range of matters regardless of the seriousness, an issue that has yet to be fully explored within a policing context. However, the introduction of Investigatory Powers Commissioners Office (IPCO) to provide independent oversight of surveillance requests and a new Home Office definition of 'serious crime' (*Investigatory Powers Act 2016, S.269(1)*, p.217) has assisted in progressing the legislation forward.

In the absence of fitting legislation to control and manage surveillance activities across social media forces introduced formal policies and strategies for its use in investigations or as evidence (Bartlett *et al*, 2013, p.5). The College of Policing Code of Ethics provides a rudimentary stance stating, 'standards that apply to the management of information off line are equally applicable to social media (College of Policing, 2014b, p.2). Yet, provides

little guidance to define the boundaries of conducting online investigations, an issue addressed in the Chief Surveillance Commissioner's annual report 2013/2014 cited in MPS (2014c, p.7) where they consider a common-sense approach by looking at the issue of 'repeat viewing' stating;

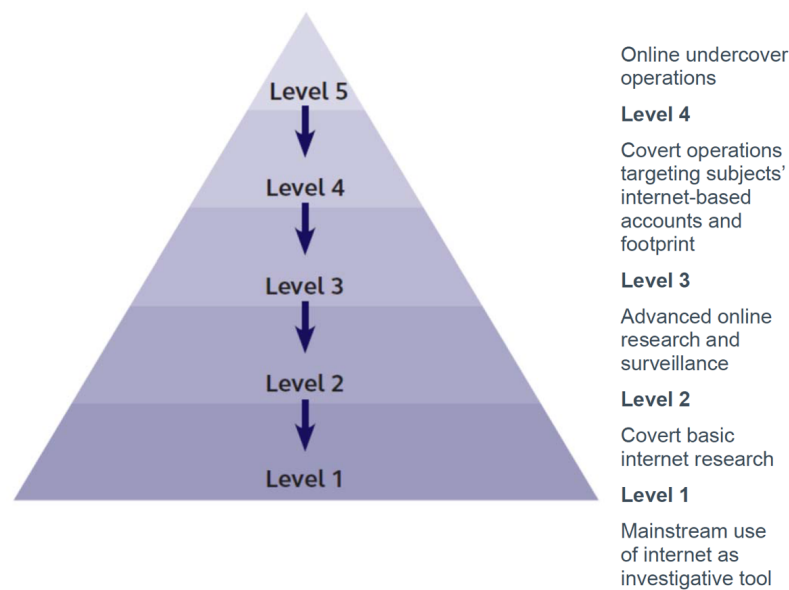
'Although there remains a significant debate as to how anything made publicly available in this medium can be considered private, my commissioners remain of the view that the repeat viewing of individual 'open source' sites for the purpose of intelligence gathering and data collection should be considered within the context of the protection that RIPA affords such activity'

Consequently, MPS (2014c) provides practitioner guidance on 'repeated viewing' saying that research over the internet or social networking sites once in an investigatory capacity to establish what information exists does not fall under the definition of surveillance and, therefore, would not require a surveillance authority. However, the repeated viewing of a social networking site to monitor an individual, rather than a group, commercial or organisational website or social media page (for example to check for status changes or other activities) would fall under the definition of surveillance and would therefore require authorisation. In addition, College of Policing (2016, p.80) refers to the established 'National Internet Investigation Model' shown in **Figure 1**. and illustrates the five investigator levels established by the Association of Chief Police Officers in 2015.

Level 1 refers to most police personnel who have received no training in online covert tactics and only affords them access to any police computer to conduct open source investigations where attribution to the police is not an investigative concern. Level two (2) and beyond require training and the use of a discreet or a fully covert terminal as a

National Internet Investigation Model

Figure. 1



minimum standard and in many cases, may require an authority under the *Regulation of Investigatory Powers Act 2000*. While those trained between levels two and five (2-5) will utilise a false persona to access certain platforms, it is only at the highest level and with authority that undercover online officers will engage with other users covertly, using their established false personas. In late 2018 this model was replaced with a three (3) tier model by the National Police Chiefs Council (NPCC) streamlining the previous model to 'overt', 'covert' and 'Undercover Online' (UCOL) in an attempt to reduce confusion over the competences at each level. It is worth noting this research was based on the five-tier model from 2015 and not the 2018 model as described by Egawhary (2019, pp.93-94).

Although MPS (2014b, p.4-5) policy specifically distinguishes between the use of overt and covert police terminals for intelligence work and the restrictions on using authorised social media accounts for intelligence gathering, there is no auditable process or form of intrusive supervision to prevent officers crossing the communications/surveillance divide and as O'Conner (2015) identifies, when new technologies are adopted by the police they can have unforeseen consequences and can significantly alter police practices.

2.2. Social Media in Policing

Communication is a fundamental social dimension of human existence (Fuchs and Trottier, 2013, p.3), and its effective use is necessary to uphold the Peelian principles that support police legitimacy (Great Britain. HMIC, 2014, p.25). Police communications utilise a variety of methods to engage with the public from as face to face meetings, organisational leaflets, newsletters, newspapers, radio (OSCAR, 2017c, p.15) to television (Ross, 2014). However, with improvements in health, education, technology and living standards the public now demand more than ever that the police communicate effectively (College of Policing, 2015) and as Fielding and Caddick (2017, p.4-5) state, 'traditional' methods have made way in favour of social media in a 'post truth' era of rising public scrutiny, allowing police services to foster understanding and tolerance through open and transparent communications (OSCAR, 2017a). By providing a 'virtual police' presence (Great Britain. HMIC, 2012, p.53) social media provides an innovative approach to demonstrating service effectiveness and presence in a cost-efficient way to hundreds of thousands of users (O'Connor, 2017, p.901; Picazo-Vela, *et al*, 2012; Trottier, 2015a, p.534), especially at a time of austerity (MPS, 2017, p.7) when police numbers are falling nationally (Weinfass, 2017).

Considered Europe's leaders in the use of social media (Bartlett *et al.* 2013, p.13) every police service across the United Kingdom (UK) have at least a corporate Twitter account (Great Britain. HMIC, 2012, p.10; Ashby, 2013). However, the MPS have expanded their digital presence to include a Facebook and Twitter account for every Safer Neighbourhood Team in London, giving the MPS the largest social media presence in the UK (MPS, 2017, p.3). Unlike traditional methods of communication social media can be employed in a covert investigative capacity too, providing a unique challenge for police services who need to strike the balance to ensure continued public support and legitimacy (Bartlett *et al.* 2013, p.6). Although social media presents challenges for the police, retired

Chief Constable Scobbie of former Association of Chief Police Officers (ACPO) stated, ‘the use of social media is likely to continue to grow and, on balance, the advantages of social media use by the police outweigh the disadvantages’ (BBC, 2012).

2.2.1. Social Media for Engagement

While OSCAR (2017c, p.16) identifies that traditional policing leaflets and newsletters suffered from issues of cost, distribution, frequency and had limited their geographical reach, Surette (2016) goes on to say, ‘the isolated acts of reading a newspaper or turning on the television have been replaced by the collective experience of posting, tweeting and going viral’. Hanson (2011) articulates this position agreeing;

‘Years ago, we would send out news releases, we’d hold press conferences — nowadays we can bypass all that. We just put it on our website, and then reach out on popular social media sites like Facebook and Twitter. We believe we’re hitting a bigger audience.’

According to Fisher (2012); Crump (2011, p.1) and Egawhary (2019, p.89) the first links between the UK police and social media started in 2008 when forces started experimenting with Twitter mainly through unofficial accounts, and with varying degrees of official support (The Police Foundation, 2014). As Sweeney-Burke (2015, p.16) comments, ‘social media has changed the way [society] communicates in the post-modern world and even if you are not consciously engaged, you are subconsciously being swept along in the largest communication shift in history.’ Citizens are increasingly using social media to communicate with their family, friends, colleagues, businesses and government in everyday situations (Kavanaugh, *et al*, 2012, p.480). Creating digitised, auditable information willingly provided and reinforced by peers (OSCAR, 2017) through ‘likes’, ‘reposts’ and ‘shares’ that drives competition amongst users to have the most attractive

social media presence, even if it does not altogether represent the user's reality (Fike, 2015).

It is difficult to comprehend social media's vast reach, as Fielding and Caddick (2017, p.4) conclude, 'any recital of numbers of social media users will be obsolete before this report is finished.' However, authors and academics regularly provide momentary glimpses which help demonstrate the sheer breadth of the internet and social media, with Longstreet and Brooks (2017, p.73) stating that there were 3.5 billion internet users in 2016 and the MPS (2017, p.4) documenting that Twitter currently has 317 million active monthly users who send out 500 million tweets a day, while Facebook had 1.23 billion active monthly users in 2013 (O'Connor, 2017, p.900). With continued increases digital connectivity, personal data is the currency for access, which provides innovative law enforcement the opportunity of interrogating larger quantities of 'intelligence data' (Burgess, 2018a).

In 2010, The National Police Improvement Agency (NPIA) issued guidelines to UK services formally recognising the potential benefits of social media (Williams *et al*, 2013, p.464; Crump, 2011, p.3; Procter *et al*, 2014, p.418). Although, the power of social media would only gain recognition by senior police officers during the 2011 riots (OSCAR, 2017c, p.11; Fisher, 2012; Crump, 2011, p.1; Egawhary, 2019, p.89), when rioter used 'dark social' such as Blackberry Messenger to coordinate disorder across the UK (Williams *et al*, 2013, p.461). Public information supplied directly through police social media accounts was weighted as both accurate and reliable, with OSCAR (2017c, p.15) identifying, this was the first time the police experienced 'fake news' and the impact of 'citizen journalism' (Williams *et al*, 2013, p.467; Trotter, 2010), but could dispel rumours quickly (Fisher, 2012) through established accounts.

Even with a range of guidance documents available on the professional use of social media (MPS, 2013; 2014a; 2014b; 2015a; 2017), discretion and trust is placed upon individual officers to communicate on an unprecedented scale autonomously. While social media provides a platform for officers to represent the service, it creates significant organisational risk as detailed by Fisher (2012) with the potential for inappropriate tweets/posts containing sensitive information, discriminatory positions, libellous details, operational activities or comments, pictures and videos that may damage the reputation of the service (Bartlett *et al*, 2013, p.5; Sayre, G. and Dahling, J. 2015, p.254). Added concern is highlighted by Schneider (2016, p.138) who questions where the line between work and personal life is, with officers encouraged to continue public engagement in their personal time. It raises questions as considered in Association of Chief Police Officers (2013, p.4) around expectations, consistency and professionalism that may have unintended consequences that lead officers into conducting investigations via unsuitable means.

2.2.2. Social Media for Intelligence and Investigations

The Police Foundation (2014) considered the advent of social media a ‘game changer’, not only for police communications but for investigative and intelligence purposes too. MPS (2014b, p.2) acknowledges the internet is a necessary function of police work, carrying the largest amount of knowledge, information and intelligence in history. Yet while an integral part of everyday life, social media was identified as the ‘newest threat to society’ (Great Britain. HMIC, 2015a, p.7) with Press Association (2012) reporting crimes involving Twitter and Facebook have risen 780% since 2008 and expose users to increased dangers of cyberbullying, hate speech, online grooming (Clapham, 2015, p.111) and recruitment into extremist ideologies (Press Association, 2012; Great Britain. HMIC, 2015b, p.25; Hanson, 2011). Great Britain. London Assembly (2013, p.10)

acknowledged law enforcement is losing the fight against internet crime stating, ‘consideration needs to be given to the basic skills required to effectively investigate cybercrimes.’ A position Great Britain. HMIC (2013, p.30) agreed, confirming production of a range of College of Policing online training packages to assist officer’s, but an issue they returned to again in Great Britain. HMIC (2014, p.16) and Great Britain. HMIC (2015b, p.25) who report, ‘the capacity and capability of agencies to address these issues ... has not kept pace with their growth.’ Suggesting that little progress had been made to manage demand, but as O’Connor (2017, p.901) states, ‘the police could not have foreseen the impact these technologies would have on resources and crime, especially given the speed at which social media has been adopted.’

In many instances’ individuals can be found online in plain sight using simple, open source research for virtually any social actor to see, without the individuals knowing who is looking at them or why (Trottier, 2015a, p.531). Where data is gathered and analysed by the police or other investigative agency in this way it is referred to as ‘Open Source Intelligence’ (OSINT) (Trottier, 2015a, p.531). Where intelligence is confined specifically to social media platforms this is referred to as ‘Social Media Intelligence’ (SOCMINT) (Bartlett *et al*, 2013, p.5) and defined by Bartlett *et al*, (2013, p.9) as;

‘Open source intelligence gathered from open, publicly available sources where no private information is collected about an individual, unless the user has no expectation of privacy and the methods of collection do not involve deception or interception.’

Whereas the definition provided in MPS (2014c, p.3) policy is more pragmatic providing examples of what open source can be, but interestingly omits social media;

‘Open source is defined as publicly available information (i.e. any member of the public could lawfully obtain the information by request or observation). It includes books, newspapers, journals, TV and radio broadcasts, newswires,

internet WWW and news groups, mapping, imagery, photographs and subscription databases.'

However, as considered by Hanson (2011) the use of SOCMINT as actionable intelligence will demand services utilise it effectively as it requires tolerance and acknowledgement that in many instances perceived threats may be throw away comments or opinions that present no risk to public safety. Particularly as services enthusiastically listen to 'reports of police thwarting or solving crimes based on [social media posts]' (Roufa, 2017a) there must be caution to 'the sheer volume of social data streams that generates substantial noise which must be filtered to detect meaningful patterns and trends' (Kavanaugh, *et al*, 2012, p.480). Especially as the growth of SOCMINT continues to aid investigations, prevent crimes, identify offenders and generates intelligence (LexisNexis, 2014, p.2-9) that can assist in spotting emerging events, piece together criminal networks, discern public attitudes and improve situational awareness (Bartlett *et al*, 2013, p.6). Yet while social media can be used for investigations and intelligence a distinction needs to be identified as to when this becomes a surveillance activity.

2.2.3. Social Media Surveillance

According to Bekkers *et al* (2013, p.335) social media monitoring is 'the continuous systematic observation and analysis of social networks and communities,' this increased collection of personal information in the digital sphere swells to produce 'Big Data', a term that refers to all forms of data, including transactional data, video data and waste information generated as we search the internet and surf the world-wide-web (Mayer-Schonberger and Cukier, 2017, p.52). A significant element of Big Data is social media monitoring or surveillance, with its origins in the private sector focusing on strategic marketing through research, trend scouting and consumer feedback (Bekkers *et al*, 2013, p.336). The repurposing of data by companies such as Cambridge Analytica (Greenfield, 2018; Tan, 2018) and the state according to Fuchs and Trottier (2013, p.21-22) creates a

society that is totalitarian in the double-sense of being a dictatorship of the market capitalist logic as well as a state dictatorship and believes that the interlocking of state and commercial surveillance poses considerable threats for society. 'Passive consent' has provided this surveillance gateway by becoming the norm with law enforcement surveillance systems such as licence plate readers, facial recognition (O'Connor, 2017, p.890), and social media scrapping assuming the right to capture data for commercial advantage or lawful investigations (Surette, 2016).

As Brandom (2016) reports, it is one thing when data is used for marketing purposes but when it results in people being arrested there is an obvious chilling effect; an issue London Assembly (2013, p.33) say the Metropolitan Police understands, stating excessive surveillance might stretch public confidence and raise ethical questions. As Mayer-Schonberger and Cukier (2017, p.150-157) details there have been many instances throughout history where data has been used for 'social sorting' of the population into groups and social media is significant to policing, as surveillance today according to Lyon (2003a, p.1) uses data to sort people into categories and could facilitate mass social sorting into general categories of 'criminal' and 'non-criminal' based on their social media profiles and posts. These are issues not only of importance to the MPS but policing nationally and through an analysis of MPS social media surveillance practices make recommendations to improve national police practice and policy.

In summary the literature agrees that there is increasing use of social media surveillance tactics by law enforcement agencies around the world. However, discussions are limited to external observers and academics who have had little or no opportunities to research the internal practices of police services in their use of social media as a surveillance tool. As a consequence, discussions as to the impact surveillance has are concentrated around theoretical perspectives and are inclined to focus on the macro scale relationships between

the police and public in the context of surveillance measures. This is reflected in the hierarchical terminology used in discussions such as, policing, government, national and global contexts and is echoed in theoretical discussions that focus on the impact of societal surveillance. Generally, literature attributes social media surveillance techniques as high-level skill sets that are only accessible to trained specialist teams such as the Internet Investigation and Intelligence (i3) Unit within the MPS who are equipped to carry out a range of online surveillance activities. What the literature fails to consider in any depth is the micro scale, the working practices of officers on the front line and how their practices influence the theoretical landscape.

Having regard for the available literature in this study the following three aims have been established:

- 1. To establish what the current social media practices being employed by policing personnel across the MPS and determine whether they constitute a form of surveillance.**
- 2. To establish whether any identified practices highlight gaps in current policy.**
- 3. Deliver a new theoretical interpretation of surveillance in the context of social media and policing.**

Chapter 3. Methodology

3.1. Introduction

This chapter outlines the methodological approach taken in this study. The research design employs a mixed methods strategy to data collection through the use of focus groups with operational police personnel (Police officers and Police Staff) who have experience and knowledge of social media practices. These focus groups provided qualitative data and a representative sample to pilot the survey in order to evaluate structure and question modification (Ruel, Wagner and Gillespie, 2016, p.101) before its full Metropolitan Police Service (MPS) wide distribution. The survey quantified what social media surveillance practices were being employed across the MPS and used qualitative questions to explore the underlying factors that legitimise police personnel's use of social media in this context.

The chapter begins by considering the role of the researcher as a policing practitioner before exploring the philosophical foundations that this study is built upon. The research design follows with details of the methods employed, specifically focus groups and survey with consideration given to their deployment, data collection, analysis, participant selection and ethical considerations. The chapter will then conclude with personal reflections of this research.

3.2. Police Research

It should be noted that the research is being conducted by a serving police officer of the MPS. As such various approaches have been considered by academics to characterise police and public sector research with Brown (1996, cited in Davies, 2016, p.158) distinguishing four types of researcher based on their affiliation with the police. These categories are defined as 'insider-insider', research that is conducted 'by' serving police officers. 'Outsider-insider' research where police officers conduct research 'on' the

service but from outside, perhaps as former officers moving into academia. 'Insider-outsider' researchers who have been hired to work 'with' the police and 'outsider-outsider' researchers with no affiliation to the police but whom are studying the police or policing. Alternatively, Fox, Martin and Green (2007, p.2) consider the position of the 'practitioner researcher', a practitioner working in the public sector and in their professional capacity undertakes research with a focus on the real problems that individuals or organisations face.

This research falls into the category of both 'insider-insider' and 'practitioner' research as it is being conducted in house 'by' a serving police officer of sixteen (16) years' service. While both 'insider-insider' and 'practitioner' research have been criticised over concerns that narrow management can evade recognised academic research techniques and is merely considered 'professional development' (Tripp, 2005, p.446). There is growing recognition that police research has reached a pivotal point, as inside practitioners under the auspices of evidence-based policing become increasingly equipped at conducting scientifically-grounded research (Davies, 2016, p.156).

During the course of this study the data collection was achieved in collaboration with Met Intelligence and the Horizons Team as they were considering similar research questions. This added another dynamic to the 'insider researcher' paradigm and as considered by Campbell (2013, p.2) not having any direct affiliation with the Horizons Team represented a partnership between practitioner and external researcher that embraced the idea that a 'stranger might be better placed to see the kind of things which, to the insider, are too mundane, too obvious, to register as an important factor' (Denscombe, 2014, p.128). Holding this position assisted in addressing issues of reflexivity raised in practitioner research, however as a research practitioner insight into front line policing

practices had a benefit in the overall research design (Fox, Martin and Green, 2007, pp.80-81).

3.3. Philosophical Perspective

Research paradigms address the philosophical dimensions of social science (Wahyuni, 2012, p. 69), they refer to theoretical frameworks of thought that act as a template or example to be followed (Miller and Brewer, 2003, p.220). As basic belief systems or worldviews they guide the investigator and impact how the research is shaped (O’Rielly, Ronzoni and Dogra, 2013, p.161), not only in choice of method but in ontologically and epistemologically fundamental ways (Guba and Lincoln, 1994, cited in Tang and Joiner, 2006, p.61). The two paradigms that underpin social science research are ‘positivism’ and ‘interpretivism’, where ‘positivism’ is the application of the empiricist model of natural science to the study of society and usually characterised by quantitative approaches that test hypotheses (O’Rielly, 2009, p.163). While in contrast ‘interpretivism’ uses qualitative research methods and believes in a fundamental difference between natural and social sciences (Tashakkori and Teddlie, 2010, p.90). However, in modern academic practices, researchers have become more flexible and can combine various methodologies to conduct their research (Plano Clark and Ivankova, 2016, p.3), leaning towards social constructionist approaches that maintain there is no ‘right answer’ waiting to be identified, instead arguing that the researcher and researched are actively engaged in constructing the world being studied (Laws, Harper and Marcus, 2003, p.273).

Plano Clark and Ivankova (2016, p.81) recognise that given the variety of research approaches available it is important to justify the chosen methods in any particular research situation and that whether a positivist, interpretive or a mixed methods approach is utilised depends upon the nature of the question(s) being investigated (Kincheloe and Berry, 2004, cited in Jackson 2013, p.57). Thomas (2003, p.2) describes quantitative

research as tending to be based on numerical measurements that generate general descriptions and quantitative research as seeking explanations for human behaviour that can be generalized to other persons and places. Both approaches add value to the examination of current social media surveillance practices within the MPS, calling for a mixed methods approach that can quantify the existence of the phenomenon while exploring the reasons that underpin the human behaviour behind it. Wahyuni (2012, p.69) emphasises the importance of questioning the research paradigm to be applied, as their ontological perspective and epistemological position frame the decisions around the intended research design. As advocated by Given (2008, p.578) research must consider the social ontology; it is not enough to focus solely on quantifying a phenomenon, even though it will uncover important data about social dynamics and patterns of behaviour. To avoid naïve empiricism, the researcher must ask how the social reality came to be constructed as it appears. In this study the question of what constitutes surveillance practices requires a deeper understanding through the behaviours' and cogitative processes involved, not only on an individual basis but as a collective representation of the MPS. Through the use of a mixed methods research design the use of quantitative methods will generate objective and measurable data, while qualitative methods will embrace a subjective and interpretive understanding of the ontology of social media surveillance within the MPS.

Jackson (2013, p.53) states that researchers' ontological stance is linked to their epistemological perspective which pertains to the knowledge of the world being researched and that an ontological view of knowledge as 'subject to interpretation' means, epistemologically, that knowledge is arrived at through sense-making and meaning, rather than through objective observation. Having considered the ontological perspective of this study with MPS personnel representing a distinct group with shared experiences, understandings, interactions and cultural interpretations that create meaningful properties

in their social world, and that as an 'insider-insider' researcher of the MPS I share and impact the nature of that reality. My epistemological position is that a legitimate way to collect data for this research is to utilise a mixed methods approach which will produce a complete picture of the social media surveillance phenomena being studied. This is more meaningful than utilising the individual components of the separate methodological approaches (Bickman and Rog, 2009, p.287). This research supports Sherman (2013, p.14) view that the finest evidence is a blend of individual experiences with the best quantitative and qualitative evidence available.

3.4. Research Design

3.4.1. Research Method

Having decided upon a mixed method approach, combining the use of quantitative and qualitative methods, consideration was given to the different approaches suitable for obtaining the primary research in this study (Greener, 2011, p.2). Morgan and Hoffman (2018, p.5) describe qualitative research as intending to understand, describe and explain phenomena ‘from the inside’ through everyday practices experienced by individuals or groups. Focus groups according to Liamputtong (2011, pp.4-5) provide the opportunity to appreciate the way people see their own reality and explore what they think, how they think and why they think the way they do about the issues of importance to them. They allow the researcher to capture shared lived experiences and uncover aspects of understanding that remain hidden through more conventional in-depth interviewing methods. Willis (2016, p.360) also states that focus groups are a good conceptual development method for survey questionnaires with Morgan and Hoffman (2018, p.251) agreeing that the success of the quantitative portion of the research depends on having materials that work well for the participants with focus groups commonly assembled to pre-test surveys prior to full dissemination. This pre-testing phase can serve to improve research validity by ensuring the questions asked truly measure what they intend to. Equally the process offers as an opportunity to measure consistency of answers across the survey questions in order to improve reliability (Ruel, Wagner and Gillespie, 2016, p.118).

Surveys according to Ruel, Wagner and Gillespie (2016, p.2) are a highly effective method of measurement in social science research with web-based surveys becoming the primary vehicle for distribution and data collection. Although more commonly used for quantitative research to generate numerical data for statistical testing and drawing inferences from a sample to be applied to general populations; surveys are also used in

qualitative research to obtain profound understanding of particular demographics (Toepoel, 2016, p.3). However, they have begun to embody an approach that can facilitate the simultaneous collection of both quantitative and qualitative data within in a single research study (Hewson, Vogel and Laurent, 2016, p.47). A concurrent design that collects qualitative and quantitative data at the same time was favoured in this study over a sequential approach as it represented a less time intensive method of data collection in a single phase (DeCuir-Gunby and Schutz, 2017, p.89-93) that suited the demands of the research questions and the sample population being surveyed.

Interviews according to Gubrium and Holstein, (2001, p.85) drive interpretation and allow for ‘cultural inferences’ and themes to be drawn from the thick descriptions obtained. In this study, ‘key informant’ interviews (Given, 2008, p.524) were considered to provide understanding and interpretation of social media surveillance at the organisational level. The use of semi-structured interviews was determined the most suitable approach to obtain descriptions of interviewee’s world with respect to interpreting the meaning of the described phenomena (Kvale, 2007, p.8). However, Morris (2015, p.7) identifies the limitation of interviews which include accessing interviewees who can subsequently present inaccurate information and data that cannot be generalised across a population. In turn dealing with participants’ recollections that appear contradictory, inaccurate or not truthful will impact on the reliability of the method as considered by Roulston and Choi (2018, p.240). In addition, they are time consuming to arrange, conduct, transcribe and analyse which can be costly (Morris, 2015, p.121). For these reasons’ interviews were considered unfeasible within the times scales and beyond the scope of this study. Observational methods were also considered but discounted, as Guest, Namey and Mitchell (2013, pp.83-84) identify they have limitations in terms of event unpredictability, time constraints and practitioner sensitivities around openly discussing and justifying practices. This type of ethnographic approach would also

fail to provide an insight into the scale of the phenomena (Greener, 2011, p.74) across the MPS.

The use of mixed methods research ‘offers a solid methodological foundation that creates an integrated approach to address complex problems of a practical nature’ (Ivankova, 2015, cited in Ivankova and Wingo, 2018, p.979). Morgan (1993, p.119) confirms the research strategy in this study stating, ‘incorporating a qualitative approach, represented by the focus group method, into an integrated research design with a sample survey component can enhance the quality of the resulting analysis and the confidence that can be placed in it.’ Employing a mixed methods design will provide qualitative data through focus groups that explore the wider cultural context of the research; while surveys employing a combination of quantitative and qualitative questions will detail whether practitioners are using social media for surveillance purposes along with the how and why they are doing it.

3.4.2. Reliability and Validity

The importance of conducting research in a way that allows the reader to have confidence in the soundness of the methodological approach should not be underestimated and the researcher should have regard for the impact of ‘reliability’ and ‘validity’ throughout the research. It is widely supported that reliability relates to the probability that repeating the research procedure or method would produce identical or similar results. It provides a degree of confidence that replicating the process would ensure consistency. Whereas the concept of validity is used to judge whether the research accurately describes the phenomenon that it intended to describe with Bush (2012, p.81) concluding that, ‘research design, methodology and conclusion all need to have regard to the validity of the process.’ As this research employees a mixed methods approach with a combination of qualitative and quantitative methodologies, a process of triangulation will be employed in the

discussion and conclusion to enhance the validity of the research findings as identified by Mathison (1988, p.3) cited in Flick (2018, p.527);

‘Good research practice obligates the researcher to triangulate, that is, to use multiple methods and data sources to enhance the validity of the research findings ... it is necessary to use multiple methods and sources of data in the execution of the study in order to withstand critique by colleagues.’

Denzin (1979, p.304) describes two alternative types of methodological triangulation as within-methods and between methods triangulation. In this study the use of surveys will employ both qualitative and quantitative responses representing a form of within-methods triangulation. While the survey method will also be triangulated against the qualitative research collected through focus groups and represent a between methods approach. Denzin argued that by ‘playing off methods against each other’ would improve the validity of the research and though the implementation of several methods the research increased reliability as ‘several methods were more reliable than one.’ Flick (2018, p.531) challenges this interpretation of triangulation stating that triangulation aims to critically question data produced by a specific method and concludes an alternative version of triangulation that refrains from testing the validity and reliability of the data and findings. Rather it examines the way that something in the social world is turned into data by a specific approach. This will be of importance later when discussing the implications of the survey distribution and the decisions around the methodology undertaken. Ultimately triangulation aims to extend insights into a subject but has deeper links to the theoretical perspectives underpinning methodical approaches which impact the reliability and validity of the research.

Through the analysis process this research seeks to draw internal consistency and demonstrate reliability using the split-half test. While there are a number of approaches

to test reliability in survey questions as considered by Litwin (1995, pp.5-32) the split-test is the most appropriate for the methodological design of survey distribution implemented in this research. Other options discounted included the Test-retest and Intraobserver methods which were unsuitable as the survey was distributed anonymously on a self-selection basis making it impossible to retest the same respondents at a later date. Alternate-form reliability was also dismissed due to time restrictions and complications it presented around distribution and length of survey. The split-half test is a suitable test for reliability given the number of respondents to the survey (n=785) and supports the methodological design employed for its distribution. They are also useful when the researcher has a theory on which the outcome should be preferred (Lavakas, 2011, p.834).

The use of focus groups over interviews was not only a conscious decision based on time constraints. As Morgan (2019, p.22) challenges the belief that individual interviews provide some sort of 'gold standard' for accuracy and validity, calling it questionable and arguing that they fail to consider the potentially heightened influence a researcher has on an individual interviewee compared to the 'strength in numbers' that comes from interacting with peers in a focus group. Additionally, while it is suggested that caution should be given to attitudes expressed in the group context, the researcher should treat those attitudes as relatively flexible constructs that are situation dependent, a feature that will be discussed in the coming chapters to interpret some of the focus group content.

3.4.3. Phase One - Focus Groups

For the first phase of this study focus groups were conducted with police personnel from across the MPS to provide an insight through qualitative content into what social media practices are taking place organisationally and whether those practices can be considered

surveillance. Participant selection was based on suitability for the issue being investigated and who would provide the best information (Liamputtong, 2011, p.51). A sampling strategy utilising inclusion and exclusion criteria drove participant selection (Given, 2008, p.743) which favoured police personnel with operational access, experience in the use of social media and those specifically authorised to only use social media for communication purposes rather than investigation or undercover activities. Consideration was given to the inclusion of officers with covert open source experience, but they represented a demographic with authority to conduct covert investigations. As the study focuses on the practices of front-line personnel who are not trained to use social media for covert activities this group was excluded from participant selection.

Within the MPS each borough has a dedicated social media officer, they are front line personnel and have direct contact with officers utilising Twitter and Facebook across their geographical area of responsibility. The sample represents experienced practitioners in the field of social media and policing who are afforded a unique position with insight to both positive and negative practices across the organisation. As the single point of contact (SPOC) for training and content creation, they advise colleagues on the appropriate use of social media and represent the target demographic capable of providing the ontological perspective required. The selection of these participants supports the use of focus groups as a purposive sampling method that uses information-rich cases to generate the best data (Borkan, *et al*, 1995, p.578).

Utilising a list of the social media SPOCs obtained from the Department of Media and Communications (DMC) provided quick and inexpensive access to the target demographic (Mariampolski, 2001, p.125) and represented an existing group from which to recruit from (Curtis and Curtis, 2011, p.110). As part of the 'recruitment plan' (Liamputtong, 2011, p.57) consideration to venue, location and timing was given to

maximise participant attendance prior to the circulation of a standardised invitation to each of the thirty-two SPOCs. As suggested by Given (2008, p.3) focus group invitations outlined purpose, participant suitability and the extent of participation required. They included location, session duration, itinerary summary, an endorsement of confidentiality, and that identities would be anonymised prior to research publication. As participants were serving police officers and staff the provision of a monetary incentive to attend would be inappropriate but money isn't everything and so participants, as social media and policing experts were incentivised using a subject matter of interest to them and the prospect of meeting fellow practitioners in their field (Tuckel, Leppo and Kaplan, 1992, p.17).

Each of the three focus groups lasted approximately an hour and thirty minutes, attracting seven to eight participants; with small groups favoured as the participants were highly involved with the topic of a potentially controversial nature. As stranger's, data pollution was avoided and groups represented a controllable size that captured a good range of responses (Guest, Namey and Mitchell, 2013, p.176). Alderson and Morrow (2011, pp.100-101) hold consent as central to the act of ethical research and link it to the provision of information so that participants can ask questions prior to the commencement of the research. Frey (2018, p.822) formalises consent as 'an agreement made with individuals to participate in research, having been fully advised of the potential benefits, risks, and procedures or activities of research participation'. In this study participants were provided with an information sheet (See Appendix B) at the beginning of each session which was read aloud to ensure understanding. It detailed the research being undertaken and key facts participants needed to know that ensured they provided genuine informed voluntary consent and allowed an opportunity for questions to be raised and addressed in the open forum. Consent forms documented participants understood the information sheet, agreed to the recording of sessions and that their participation was

voluntary and confidential. However, while the researcher can protect confidentiality and anonymity within the methodological approach and appropriate management of data, it was highlighted to participants via the information sheet that no such guarantee could be afforded to the potential of other participants disclosing information obtained during the focus group (Morgan,1993, p.12). Upon acceptance of the information, consent forms were signed by the researcher and participant, duplicated and provided to both for record keeping (See Appendix C).

To ensure continuity across focus groups a 'Focus Group Plan' was adhered to, (See Appendix A) dividing sessions in two parts with the first employing the focus groups to pilot the intended research survey. This provided the target population the opportunity to highlight wrongly formulated research questions (Sieber and Tolich, 2013, p.125) resulting in a number of changes identified through a group debrief (Ruel, Wagner and Gillespie, 2016, p.107). These included structural amendments to questions and a requirement to improve terminology explanations around the use of 'Open Source and 'Online Investigation' throughout the survey. Modifications were tested in subsequent focus groups to ensure participant compatibility. While Kara (2012, loc 2529) suggests sending participants questions prior to the focus group to allow preparation; this study took an approach closer to Barbour (2007, p.85) by supplying participants a copy of the survey questions at the beginning of the session. Completing the survey at the outset meant it was seen by all at the same time, allowing the average completion time to be monitored and safeguarding against concerns of survey fatigue (Sue and Ritter, 2012, p.22). Hugick and Best (2008, p.660) consider questionnaire length and identify it a major factor if it exceeds twenty (20) minutes. In this study respondents were time and took no longer than twenty (20) minutes to complete the survey. The pre-test survey was paper based, and suggested that the final survey, being internet based and containing elements of automation to direct respondents seamlessly and logically through the survey would

therefore reduce the questionnaire length further. In addition, the provision of stimulus material (Barbour, 2007, p.85) provided participants the opportunity to become cognitively attuned to the issues surrounding social media in a policing context and consider their own ontology before engaging in group discussion. Although the second session intended to provide a separate dialogue around the use of social media for surveillance; group communication meant as moderator it was necessary to balance enforcing the intended plan against the qualitative benefits of allowing participants to freely interact and express themselves (Gubrium and Holstein, 2001, p.146). Adopting Barbour's (2007, p.99) flexible approach to the application of loosely structured topic guides allowed for the acquisition of rich qualitative data that picked up new topics as they emerged and harnessed participants' insights into the subject.

Audio recordings obtained during the three focus groups were initially transcribed utilising an automated service through *Trint.com* which mitigated issues such as rate of speech, volume and overlapping speech (Paulus, Lester and Dempster, 2014, p.96) during the transcription. Liamputtong (2011, p.165) raises concerns however over paying for transcription and the subsequent accuracy of the transcription. Although the initial automated transcription removed the burden of manually typing the entire text it was subsequently compared against the original audio for accuracy and represented an initial data analysis. Verbatim and Jeffersonian types of transcription were considered but deemed unnecessary to achieve the aims of the research. Instead a condensed version of 'gisted transcription' was favoured as 'it removed unnecessary words and phrases, leaving a simplified version with the exact words' (Paulus, Lester and Dempster, 2014, p.98). The completed transcripts were then analysed using a list of basic questions suggested by Flick (2006, p.300 cited in Liamputtong, 2011, p.174) that qualitative researchers use as a coding strategy (See fig.2) to assist in the identification of themes across the focus groups.

Figure 2. List of questions for thematic coding strategy

What	What are the phenomena of concern/being mentioned?
Who	Who are the persons involved? What roles do they have? How do they interact?
How	Which aspects of the phenomena are mentioned/Omitted?
When	Referring to time, course and location. When does it happen? How long does it take? Where did the incident occur?
Why	Which reason(s) are provided or can be constructed?
How Much/How Strong	Referring to intensity. How often is this issue emphasised?
What For	What is the intention of the phenomena? What is the purpose?
By Which	Referring to means, tactics and strategies for achieving the aim. What is the main tactic and how is it accomplished?

Thematic analysis is one of the most common approaches to qualitative data analysis and generates key patterns identified in the data that may be important features to the phenomena in question.

3.4.4. Phase Two - Survey

The distribution of an MPS wide survey signalled the second phase of this study. Survey research is considered a highly effective method of measurement in social and behavioural science research (Ruel, Wagner and Gillespie, p.2). In this study the methodological design incorporated a singular cross-sectional survey that captures data from the target sample at a particular point in time; before forming a basis by which to infer characteristics against the population from which the sample was obtained (Jupp, 2006, p.53).

Questions were designed to maximise inclusion across the range of ontologies that exist within the MPS and the subject matter arena. As detailed by Ruel, Wagner and Gillespie (2016, p.44) the type of measures developed within the survey instrument should ideally produce, unbiased, error-free data. Therefore, setting concrete research goals was paramount to ensuring the survey answered the research questions. In this study the

survey generated an understanding of what practices are taking place across the MPS and why they were taking place in order to understand the ontology of social media surveillance within the policing context.

Modern web questionnaires offer a range of different features that cannot be achieved through traditional pen and paper designs (Fricker and Schonlau, 2012, p.1). With N=29,289 Police Officers (Inc. PC/DC N= 23,707, PS/DS N=4391 and Insp/DI N=1191), N=8,868 Police Staff and N=1228 Police Community Support Officers totalling N=39,385 police personnel as of February 2019 (MOPAC, 2019) across the 32 London Boroughs; an online non-list-based survey contained within a URL was published on the MPS Intranet page to engage the target population. Response rates to internet surveys generally receive lower returns which can impact the validity of the data (Feusch, 2012, p.380) and to address this Vehovar and Manfreda, (2017, pp.148-150) recommend a strategy of multiple contacts with the target sample to increase engagement. In this study, after the survey was placed on the intranet a communication was sent to each of the 32 Staff Officers across the MPS requesting the survey URL be sent directly on e-mail with a communication outlining the purpose of the survey to all personnel in their geographical area. In addition, a private direct message was sent through Twitter to all of the 649 safer neighbourhood ward accounts as well as the 32 borough accounts which trained front-line personnel have access to. Running the survey for 12 weeks and spreading the communications described across that period resulted in n=785 responses to the survey. Demographically the survey was intended for frontline personnel who use open source and social media resources and with PC/DCs representing 71% of respondents and Police Sergeants, Inspectors and Police Staff from bands E, D and C representing 26% the survey was received by the target sample. Only three percent (3%) 'preferred not to say' or selected 'other' as an option.

While the survey produced $n=785$ responses which would represent a confidence level of 95% against the population size, consideration needs to be given to the sample selection process. In order to effectively maintain respondent anonymity a systematic sampling structure across the MPS was not viable as this would have required specific targeting and monitoring of replies from each of the selected respondents. In addition, it would have required access to every employee's pay/warrant number in order to identify the regular intervals in the sampling frame; information that would have been very difficult to gain access to when considering privacy and security of personnel details. As a result, the survey was distributed on a self-selection basis to ensure respondent's anonymity. However, as identified by Sterba and Foster (2008, pp.807-808) this causes underlying statistical problems when the sample data is inferred against the population data and should be used as a guide rather than an exact statistical inference. Utilising the split-test reliability coefficient the responses were divided into two groups. The questions of relevance to the research were included in the test which provided a reliability coefficient of $r = 0.94$.

With this in mind it is worth noting that the key demographic in this research was frontline constables with $n=560$ represented in this survey. While caution should be taken when inferring the data statistically, the questions being asked placed the respondents in a professional quandary as the survey in parts asked them whether they were doing something wrong. Given the frequency of positive responses to these sensitive questions it can be suggested that the response rates act as a base line. As Lavrakas (2011, p.834) articulates, 'any mode of data collection that increases the number of sensitive behaviours is considered better under the assumption that respondents will underreport those behaviours.' Generally, respondents are considered likely to answer in line with accepted practices, culture and social norms of the associated group they represent. However,

Lavrakas' position adds weight that these practices are likely to be underrepresented creating a juxtaposition that the external reliability should be treated with caution even though the findings support the alternative hypothesis as they may be higher in reality.

Survey questions are measurement tools, and this study utilised a multidimensional concept to question formulation (See Appendix D) in order to achieve the research aims (Ruel, Wagner and Gillespie, 2016, p.46). Asking respondents, single concept questions such as, 'do you use social media for surveillance purposes?' would unlikely yield truthful results given its provocative stance or provide sufficient detail to understand the 'why'. Instead the first section considered levels of training, uses of social media and awareness of different ways to conduct investigations across social media which once interpreted answer the fundamental research question. As considered by Holyk (2008, pp.657-658) open-ended questions that test respondent's knowledge base were used sparingly and chiefly towards the end of the survey as they are cognitively demanding on the respondent. While closed-ended questions with predetermined response categories were used to enable the comparison of respondents and focused towards the beginning of the survey to ease participants into the survey and encourage survey progression. As considered by Ruel, Wagner and Gillespie (2016, pp.56-61) a combination of fixed-choice question types were used within the survey depending on the nature of information being sought from the respondent. These included multiple choice questions where clear and unambiguous options were provided to the respondent, for examples;

1. To what level are you trained in Online Investigation (Open Source)?

- | | |
|---|--------------------------|
| Level 1 (Not specifically trained) | <input type="checkbox"/> |
| Level 2 (Core Open Source Investigation/Research) | <input type="checkbox"/> |
| Level 3 (Advanced Open Source Investigation/Research) | <input type="checkbox"/> |
| Level 4 (Network Investigations) | <input type="checkbox"/> |
| Level 5 (Undercover Officer online, Covert Internet Investigator) | <input type="checkbox"/> |

Rating scale questions that used responses to represent a continuum from which respondents choose the single best answer, for example;

4. Approximately how often do you use Online Investigation (Open Source) research in your work?

- Very frequently (several times a day)
- Frequently (1-2 times a day)
- Occasionally (2-3 times a week)
- Rarely (2-3 times a month)
- Very rarely (once a month or less)
- Other (please explain):

Finally, checklist questions were used when it was important to allow the respondent the opportunity to select multiple responses, for example;

7. How have you conducted Online Investigation (Open Source) research? Please tick all that apply.

- Request submitted to Open Source Unit
- Request submitted to LIT
- Request submitted via CRIMINT
- Used an Aware terminal (MPS desktop computer / tablet device etc.)
- Used a Covert terminal (standalone, not overtly linked to the MPS)
- Used my personal, non-work-related device (your own phone/tablet etc.)
- Other (please explain):

Where appropriate in ‘rating scale’ and ‘check list’ questions comprehensive lists were drawn up of potential answers followed by the option of ‘other – please specify’ to capture answers not thought of by the researcher in survey design. Litwin (1995, pp.1-4) discusses psychometrics in survey design questions and raises the need to ensure that surveys ask questions in a way that demonstrate reliability by eliciting the same kind of information each time they are asked. Therefore, consideration was given to ‘rank order scales’ where respondents put choices in order themselves and ‘Likert scales’ where participants are asked to indicate their agreement or disagreement with a statement but were discounted as they would not provide the necessary reliability sought through the survey questions.

Demographic questions provide a clear picture of who participated in the survey and assist in making arguments around generalisability of the sample to larger populations. Consideration was given as to their placement within the survey as they can invoke sensitivities that impact survey completion (Allen, 2017, pp.2702-1704). In this study the three demographic measures considered relevant were age, length of service and rank; these demographics provided a base for correlation against practices that aids in

presenting generalisations around social media surveillance practices within the MPS. Some of the established demographics in survey research such as gender (Ruel, Wagner and Gillespie, 2016, p.45) and ethnicity were excluded from the survey on the basis of relevance to the research questions and to further prompt the notion of anonymity. While Givens (2008, p.847) suggests sequencing demographic questions towards the end of the survey to maximise respondent engagement, they were placed prior to the final four (4) questions in a strategic decision based on the value of demographics data verses the benefit of the data obtainable in the final knowledge section. Questions 1-4 in the final section evaluated respondent's knowledge of legislation, policy and ethics in relation to open source investigations, and combined fixed-choice typology with an open-ended option, for example;

1. Does the Regulation of Investigatory Powers Act (RIPA 2000) impact the way in which police obtain Online Investigation (Open Source) intelligence?

- Yes (pop up) Please briefly explain why **(TEXT – Max 1000 words?)**
No (pop up) Please briefly explain why **(TEXT – Max 1000 words?)**
Don't know

This was used so encourage participants to commit to an answer and then explain their understanding if they could, generating a detailed picture of participant knowledge within the sample. By placing these cognitively complex group of questions at the end of the survey eighty-three percent (83%) of respondents completed the entire survey. Caution should be taken in relation to the validity of these questions as they do represent complex topics that require further analysis and research in their own right.

Focus group participants (see phase one) were used to test and discuss the survey questions prior to full dissemination across the MPS (Holyk, 2008, p.659). Consequently, changes were made to the wording of questions including question 1. which asked; 'To what level are you trained in online investigation (Open Source)?' While officially the levels are one-to-five (1-5), with one (1) formally recognised as 'overt open source

investigation/research' this caused respondents confusion as it suggested a minimum basic level of training that most had not attained.

Participant: *'The first question, is that level one (1)?*

Facilitator: *'Yes level one (1) is the basic level with no training.'* – Focus Group 2

Participant: *'That took a little bit of reading to figure out.'*

[Group agrees with member that the first question needs clarification] – Focus Group 2

As a consequence of the feedback the option was changed to, 'not specifically trained.' In subsequent trials respondents no longer raised the question as problematic. Focus group participants also raised concern at the use of the term 'Open Source' highlighting that they felt it was too restrictive and unclear;

Participant: *'The fact that the words 'open source' is there. It's a bit restrictive, a lot of people will step back from that.'* – Focus Group 1

Participant: *'I think a lot of people will read that, 'have you conducted open source research?' and they would think no. Open source research doesn't cover what I have done, so then you wouldn't get the answers to the next questions.'* – Focus Group 1

As a result, the terminology throughout the survey was changed to say, 'Online Investigation (Open Source)' resulting in support from the focus group that raised it;

Participant: *'People will relate to "online research" more than they can relate to "open source."* – Focus Group 1

In later focus groups trials the use of 'online research throughout the survey received no further criticism. Making these changes further ensured the reliability of the survey by ensuring participants understood question wording and were able to respond consistently as a sample to what was being asked.

Utilising 'London Voice', an online survey tool supplied to the MPS as part of the Mayor of Police and Crime (MOPAC) contract with Open Research Services (ORS) afforded

breadth of coverage to the target demographic (Denscombe, 2014, p.29). London Voice offered a cost and time efficient survey distribution method while reducing potential errors arising from the transcription of paper questionnaires (Vehovar and Manfred, 2017, p.143). In addition, it safeguarded participant anonymity externally of the MPS due to the Data Sharing Agreement (DSA) which ensured all data uploaded was only shared as agreed with the MPS, not disclosed to third parties and secured any ‘paradata’ obtained during the respondent’s completion of the survey (Toepoel, 2017, pp.184-186). Due to the sensitive nature of some of the questions addressing anonymity internally of the MPS was equally important and was raised during the focus group sessions;

***Participant:** ‘Anything that says anonymous; there will always be officer cynicism.’ – Focus Group 1*

***Participant:** ‘Unless the DPS (Department of Professional Standards) send out an e-mail themselves saying its completely anonymous, we are a cynical bunch [Police Officers] and it doesn’t matter what you say, we will always think that someone is looking’ – Focus Group 2*

Highlighted by Allen (2017, p.228) that reassuring participants of their anonymity is essential to building trust between the researcher and voluntary participant so they can feel comfortable completing the survey. Researchers have a responsibility to keep participants safe from harm, embarrassment or repercussions from employers and in this study serving police personnel were being asked about their involvement in practices that could raise ethical and professional questions. As a consequence, anonymity was addressed at the outset in the survey through the information sheet and at key points during the survey the word ‘anonymous’ was written in bold and highlighted in red to cognitively remind participants of their anonymity, especially around questions that may be considered sensitive.

In addition, the information sheet as considered by (Ruel, Wagner and Gillespie, 2016, p.25) contained details of who the survey was for, the purpose of the survey, key definitions to help participants, the authority to conduct the research, rationale for collecting participant demographics, how participant information and responses will be used and finally how to contact the researcher directly if questions arise. Providing this information increases participant confidence in the survey legitimacy and serves to further reassure respondents that their identity remains anonymous, whilst ensuring informed voluntary consent.

The quantitative survey results were then analysed through SPSS, while the qualitative results from both the survey and focus groups were analysed through NVIVO with the triangulated analysis (Given, 2008, p.527) identifying social media surveillance practices within the MPS, a gap in current MPS policy and providing characteristics to establish a new theoretical interpretation of social media surveillance.

3.4.5. Ethical Considerations

There were a number of influences that required reconciling prior this studies commencement to guarantee it met CCCU's ethical standards. As Fox, Martin and Green (2008, p.103) identify practitioner research may highlight inappropriate practices or organisational failures and inadequate participant anonymity at the outset could create a research environment where 'organisational influence' informs participant contribution or hinders involvement altogether. As a policing practitioner conducting insider research, it was identified at the outset that researching social media surveillance with police personnel may plausibly uncover inappropriate practices. This then produced an ethical conflict with the 'Police Code of Ethics' that governs policing (College of Policing, 2014b). Firstly, the codes dictate that police officers should act confidentially, 'treating information with respect, accessing or disclosing it only in the proper course of their

duties'. Creating a dilemma for both the researcher and participants in their ability to openly share information about policing practices for research purposes. Secondly officers are bound by the codes to 'report, challenge or take action against the conduct of colleagues which falls below the standards of professional behaviour', creating an expectation that identified wrongdoing is challenged or reported. These issues were raised with MPS HQ Strategy and Governance Unit and the College of Policing who recognised the challenges of social research within policing contexts and support the research being conducted as recorded on the 'Information Sheet' for the information of participants. Brunger, Tong and Martin (2016, p.198) consider the ethical challenges of policing research in detail and articulate that a number of factors need to be considered when weighing up a particular ethical dilemma. These include established agreements of confidentiality and anonymity with participants, practitioner codes of ethics, organisational powers and policies, as well as university and research governance which will affect the researcher's instincts of right and wrong. Of equal importance is the organisational risk that conducting this research generates and whether proceeding outweighs the potential exposure of inappropriate practices. In this sense any results would lead to greater awareness of the cultural practices surrounding the use of social media surveillance in a policing context, allowing for informed policy and practice development to safeguard police services, officers and the public from the potential dangers of social media surveillance in the future.

According to Dingwall and McDonnell (2015, pp.153-154) human participants should not be exposed to unnecessary risks of harm and it is the responsibility of the research team to assess and manage potential risks within their study. In this study the focus group sessions and the survey were subject to a risk assessment in accordance with CCCU health and safety practices (See Appendix E). The risk assessment considered the following;

1. Physical risk.
2. Psychological risk resulting from discussing potentially inappropriate practices of social media surveillance.
3. Genuine voluntary consent.
4. Confidentiality and Anonymity.
5. Breaches of Professional Standards.
6. Reputational Damage to the MPS.

A risk matrix incorporated within the CCCU health and safety procedures evaluated the severity of risk against likelihood which concluded a low probability of their occurrence in this study and that if they did occur the impact would be minor. Risks four (4) to six (6) received a slightly elevated likelihood score due to the nature of the phenomena being researched and potential impact on individual participants and/or organisational reputation. However, the risk assessment for each phase of the study remained within the low/acceptable range and therefore necessitated no further action or mitigation but required continued observation to ensure no increase in the risk throughout the duration of the study. Completed risk assessments were subsequently included as part of CCCU's Ethics Review Checklist (See Appendix E) for consideration by CCCU Ethics Review Panel. This study involved, 'the discussion of, or collection of information on, or topics of a sensitive nature' such as police practices and culture in the use of social media as a surveillance tactic and therefore required a full ethical review. The Ethics Committee evaluated the study and found that it met CCCU's ethical compliance standards (See Appendix F).

3.4.6. Personal Reflections

As my first experience in academic research this has challenged me on more than one occasion. Over the last three years there have been a number of obstacles to overcome

professionally, academically and personally to ensure this research was completed as detailed in my research timetable (See Appendix F).

From the beginning I was aware that conducting this study would be time consuming and endeavoured to have a proactive attitude towards conducting the research within the two-year timeframe. Around the same time as undertaking the 'Masters by Research' programme I began a new role as the Social Media Engagement lead for Ealing Police; it was a result of accepting this role that I began to establish the initial research questions for this study. Shortly after beginning the programme the opportunity to apply for a bursary through the College of Policing arose and participating in the application process led me to a chance communication with a colleague from Met Intelligence who had also been awarded an academic grant. This provided an opportunity to develop my research proposal further and ascertain that a unit within Met Intelligence, the Horizons Team were about to engage on a piece of work looking at the same subject matter.

While this provided a valuable opportunity to work in collaboration with the Horizons Team, it quickly became a necessity so that similar research wasn't being undertaken by two different entities at the same time. By working in partnership, it prevented duplication of effort and reliability concerns over attempts to obtain similar data sets from the same target sample. While there were clear advantages to data acquisition by working together it was a challenge in the beginning to ensure that expectations were laid out from both sides to ensure a cohesive working relationship. This included making a stipulation at the beginning that all data collection methods had to comply with CCCU research ethics criteria to ensure that the study met the necessary standards. However, while these negotiations were relatively straightforward, the Horizons Team had stringent timeframes for the data collection which caused challenges around my original research schedule. In order to manage the tight timeframes, I brought forward the focus groups and survey

deployment which increased the pressure on me to complete the literature review within the proposed schedule.

However, these challenges were met by rearranging the original schedule and taking time away from work to ensure research tasks remained on track. At an early stage of research design, it became clear that there was an ethical issue that needed considering. To ask operational police personnel if they have been working outside of approved police practice would create a number of issues for me both professionally and academically. In order to overcome these concerns dialogue was established with both MPS HQ Strategy and Governance Unit and the College of Policing who respectively permitted the research to proceed and supported it through the bursary scheme. In order to further satisfy any ethical concerns, the research was submitted for a full ethical review through CCCU.

The focus groups were straight forward to organise but with little experience in moderating a focus group, the first resulted in me talking too much to fill gaps of silence. By the second and third focus groups, I had established a rhythm to keep topics and conversations more focused and allowed silences to be filled by the focus group members, making for a smoother flow in the conversation. In relation to the survey I had concerns around the number of questions and the ability of this research to manage the volumes of data they would generate. Some of the questions were specifically necessary to the Horizons Team but in pretesting none of the participants raised the number of questions as an issue and so the survey was left unaltered in this regard. Originally the survey was only going to be accessible for six (6) weeks but this time frame ran across the Christmas and New Year period of 2017/2018. In retrospect the delivery timeframe was not ideal but internal pressures to push the survey out meant this was a compromise that had to be made. However, a review of the number of completed surveys in January 2018 led to further discussions with the Horizons Team and an extension until March 2018 with

additional direct engagement to encourage participation in the survey. Had time allowed and in hindsight I would have altered the methodological approach to sample selection and considered ways to make the sample process more systematic rather than self-selection. This would have allowed for a more precise inference of the final results against the research population, reduced the effects of sample bias and improved the external validity of the research (Lavrakas, 2011, p. 347).

Once the data was acquired it was shared with the Horizons Team who benefitted from the academic rigor provided by working in partnership with a postgraduate student. In addition, working with the Horizons Team allowed me the opportunity to engage with open source practitioners, and develop a greater understanding of how open source and social media are used within a policing context. In April 2018 a Sergeant's position on the Horizons Team became available and given my close working relationship with the team it felt like the right opportunity. I applied and detailing the research work that I had completed to date with the team and was successfully appointed in the role. While this was a fantastic opportunity, starting a new job added another dimension of stress on top of selling our family home and welcoming the birth of my son Aidan in August 2018. These personal milestones created delays of approximately four months in the data processing of the focus groups and survey resulting in a (6) six-month extension to complete the research.

To conclude this reflection, I have recognised the benefit of having internal access to the sample set and while there were benefits to an internal collaboration including delegation of tasks, support in the facilitation of focus groups and deployment of survey. There were also significant challenges and compromises that have to be made such as altering schedules and managing conflicting demands that wouldn't have arisen if I were conducting the research fully independently.

Chapter 4. Results and Discussion

4.1. Introduction

The results and discussion represent the triangulation of research generated through qualitative data obtained during three (3) focus group sessions (Full Focus Groups Coding - see Appendix G) and quantitative and qualitative survey sample data collated from n=785 survey respondents (Full Survey Results, including referenced tables and figures – See Appendix H). It is worth noting that there is no similar internally produced research at this time that can be compared against the results found here. However, research produced by LexisNexis (2012; 2014) offers the most suitable comparison in some areas as it focuses on aspects of social media use in US law enforcement and where appropriate comparisons have been considered against their published data. However, it is important to note the LexisNexis research is generated for corporate benefit and their methodology impacts the data by actively implementing sample bias by only targeting respondents who use social media on the job (policing). Therefore, the data naturally reflects a high number of police personnel who use social media for intelligence, investigative or communicative purposes and discounts those who don't use social media for such reasons. This is important as the data suggests 81% of police personnel in the US are actively using social media for investigations, when in fact it is 81% of the sample and cannot be inferred as an accurate population proportion.

In this analysis it is important to recall the key definitions relating to 'open source intelligence' and 'social media intelligence' as the quantitative survey results utilise a combination of the two terms to ensure respondents understood the context of the questions and to improve reliability. Where data is gathered and analysed by the police or other investigative agencies from open, publicly available sources, where no private information is collected, it is referred to as 'Open Source Intelligence' (OSINT) (Bartlett *et al*, 2013, p.9; Trottier, 2015a, p.531). Where data and intelligence are confined

specifically to social media platforms this is referred to as ‘Social Media Intelligence’ (SOCMINT) this can be public and private information.

While the expressed and measured demographics in the survey were, age, length of service and position, questions one (1) and two (2) also represented a demographic means by which to sort the sample as respondents were asked their level of training in open source and social media. The five (5) demographics represented independent variables against which to test the dependent variables collated across the survey results which included;

Q.4. Respondents frequency of online investigations.

Q.6. Respondents awareness of the open source unit.

Q.7. How respondents conducted online investigations.

Q.7.1. How respondents used their personal devices to conduct online investigations.

Q.8. Why respondents didn’t use the services of the Open Source Unit.

Q.9. Respondents use of their personal social media accounts for online investigation.

Q.10. Respondents use of false personas to conduct online investigation

Knowledge Q.1-3. Respondents knowledge around RIPA/Policy/Ethics.

Knowledge Q.4. Respondents beliefs around privacy.

In considering these variables this research is founded on a null hypothesis that MPS personnel are generating OSINT and specifically SOCMINT within the remit of their training (or lack of training, at level one) without using their personal social media accounts, a false persona or their personal devices. The alternative hypothesis is therefore that, with no training or authority MPS personnel are utilising SOCMINT for policing activities, exploiting access through personal mobile devices, personal social media

accounts or by creating false personas to remain covert. These activities constitute a form of social media surveillance that are presented ontologically as for a 'policing purpose' by those engaging in the described practices.

The quantitative results represent a combination of descriptive statistics to evidence what practices are taking place within the sample data and inferential statistics to estimate the parameters for the MPS population. Utilising the confidence interval for population proportions formula the results can be inferred to a confidence level of 95%, while statistically asserting that there is only a 5% chance that the true population results will fall outside the confidence interval ranges.

A number of topics were identified through the data analyse that have been grouped together under three (3) overarching thematical heading; '*Social Media and the Front Line*' which evidences who within the MPS is utilising open source for intelligence and investigative purposes, examines the frequency of its use and evaluates what practices are appearing in the data. The second theme, '*Social Media in a Policing Context*' evidences what MPS personnel are looking for when using open source and social media in a policing context and explores why they engage in these practices. With the final theme, '*Policing dilemmas and Social Media*' evidencing the challenges presenting the police in the use of open source and social media and discusses the legal, ethical and organisational implications by looking at the knowledge levels of MPS personnel, before finally considering how MPS personnel view the public's online data and privacy to justify their use of it for a 'policing purpose.'

4.2. Open Source and the Frontline.

The analysis of respondents to the survey results begins with **Table 13.** (see appendix) showing the frequency of respondents defined by their grade/rank within the MPS, while **Figure 20.** (see appendix) represents the percentage of respondents by rank/grade it identifies the modal response as PC/DC with n=560 responding to the survey. This group represents a significant category in this research as frontline police officers are engaged in investigations and matters of safeguarding on a regular basis and are most likely to use open source to support that work demand. In the LexisNexis (2012) report into social media use in law enforcement the demographics also represented a higher proportion of frontline personnel engaging in the research with 55% of respondents representing 'rank and file.' **Table 14.** (see appendix) shows the frequency of respondents by 'length of service' while **Figure 21.** (see appendix) represents the percentage values of those frequencies and identifies the modal length of service as 10-15 years with 26% of respondents in this category. Those with service between 2 years and 20 years had the greatest representation making up 80.5% of the survey sample, while those with 0-2 years' service and 20-35 years made up 19.5%. The frequency is not surprising and represents the recruitment drive at the beginning of the millennium to meet the then target of 35,000 (MPS, 2003, p.9) officers. With recent austerity the numbers of new recruits is significantly lower than previous years (HMIC, 2012, p.26), while those later in service tend to be harder to reach and engage with. In the LexisNexis (2014) report respondents' length of service was only divided into four categories compared to the eight (8) categories in this research. However, there were similar trends with the LexisNexis report identifying greater responses from those with 11-15 years' service and those with 15+ years but as their categories are broader it is difficult to draw direct correlations in this demographic. **Table 15.** (see appendix) showed the frequency of 'age' groupings for survey respondents, with **Figure 22.** (see appendix) representing the percentages and identifies the modal response as 35-44, with a M=38.5 years, overall those aged between

25-54 represented 90% of the respondents in the survey, while those in the 18-24 category, 55 and over or preferred not to say represented the remaining 10%. Similarly to the length of service demographic the frequency here arguably represents the recruitment drive at the beginning of the millennium; with a reduction in recruiting in recent years highlighted by the lower representation of 18-24 year olds and naturally as personnel come to end of their 30 years' service and retire there is a drop in the frequency of those aged 55 and over. While the LexisNexis (2014) report captured age demographics using broader categories, with everyone ≤ 35 in one category and only four (4) categories in total. Interestingly they had the same modal age range as this research of between 35-44 in both their 2012 and 2014 studies. Generally, both LexisNexis 2012 and 2014's demographics are similar to those of this research and offer a good comparison in those areas of research where there is overlap.

Table 1. (see appendix) shows the frequency of personnel that are open source trained with Level One (1) respondents who have had no training in the use of open source representing the modal response $n=685$ or 87%. **Figure 5.** (see appendix) shows the percentage of personnel trained at each of the five (5) levels with reducing representation as the levels increases due to the specialism of the roles and training cost implications. However, those trained at level two (2) and beyond are authorised to utilise open source for intelligence and investigation purposes via approved discreet or covert computer terminals across the MPS estate. As with Level One (1) personnel, they are not authorised to use their personal social media accounts or their personal mobile devices to conduct any police related research. While they are permitted to utilise false personas to facilitate access onto social media platforms, it is only personnel at Level Five (5) who are authorised to covertly engage with other users online. As the complexity of the investigation or intelligence requirement increases so does the necessity for personnel to be trained beyond level two (2) and the likelihood that a Directed Surveillance Authority

(DSA) will be required, especially where there is ongoing monitoring, a likelihood of personal information being obtained or the plausibility of collateral intrusion occurring.

As highlighted in the introduction of 'Real lives, real crimes' (HMIC, 2015, p.5) those who commit digital crimes create victims. Those victims demand and deserve the support of the police as much as any other victim of crime, with the report identifying a mixed picture when considering the extent to which police officers and staff know of and are trained in digital crimes and modern technology. Yet even HMIC's understanding of digital crime appears to stop short of considering the benefits and implications of OSINT in everyday policing activities, from gathering intelligence on gangs, safeguarding the vulnerable, investigating crimes to identifying and locating offenders. The MPS was unable to provide a concrete statistic for the number of open source trained personnel, however, organisational estimates gathered in consultation with the Horizons Team suggest between 750 – 1000 personnel are trained between levels two (2) and five (5). This creates a concern with the validity of question one (1) which identifies 87% (**Table 1.**) of the sample have had no open source training and currently sit at Level One (1). According to the survey 13% of respondents are trained between levels two (2) and five (5) which is not representative of the training within the population.

However, what can be stated with certainty is that 87% of survey respondents have had no open source training and demonstrates a vacuum of skills within the service and missed opportunity in harnessing the value that open source intelligence and investigation presents to police personnel. This issue that is reflected internationally (Sampson, 2016, p.55; LexisNexis 2012; 2014) and equally fails to embrace the HMIC (2015, p.74) recommendation;

'To provide appropriate and continuing training and guidance for all those within his or her force who are likely to deal with digital crime and its victims.'

In comparison **Table 2.** (see appendix) evidences how many respondents state they have been trained in social media for the purposes of community engagement through the official MPS social media presence. There are two (2) avenues for personnel to receive this training, either officially through the Department of Media and Communication (DMC) who manage communications with the press, branding and the MPS social media presence used to engage with the public. Alternatively, the second avenue is via designated personnel across the MPS who have been trained by the DMC and authorised to deliver training locally to officers and staff wishing to use social media (Twitter and Facebook) for engagement purposes. **Figure 6.** (see appendix) shows the percentage of respondents and the various methods of social media training with the modal response for social media training being 'No Training', with n=359 respondents, while the second highest answer is 'Self-Taught', n=247, combined they equate to n=606 (n=359+247) or 77% of survey respondents who have received no official training in the use of social media. As with official open source training, the absence of record keeping means there is no immediate process of identifying how many MPS personnel have received social media training. Those survey respondents trained in social media totalled 23% (DMC Trained + Borough Trained) and would represent an estimated **N=9,000** personnel across the service. This figure is considered high as a population parameter based on official suggestions by the Department of Media and Communications (DMC) there are only approximately 2000 trained MPS personnel and suggests a failing the methodological approach used to engage survey respondents using official MPS Twitter accounts. This approach potentially increased the number of personnel participating who had training in social media. However, it still shows that the combination of 'Self Taught' and 'No Training' respondents equals 77% which represents approximately **N=29,000** personnel. This data reveals the lack of training amongst MPS personnel and is comparable to the LexisNexis (2014) report, however their report only focuses on social media training and

not open source training, it does perform a deeper analysis yet identifies that 75% of personnel are 'self-taught'. While the LexisNexis research excluded those not using social media 'on the job', comparisons can be drawn from this research that identified 31% of respondents were also 'self-taught'. 'Self-taught' represented the second highest response to survey question two (2) but when combined with 'No Training' as the two (2) answers are intrinsically entwined, the overall response rate of 77% supports the international trend that police personnel are predominantly self-teaching and generally left without support and guidance from their respective police agencies. It also highlights a correlation in the LexisNexis report that, if 75% of respondents are self-taught, yet 81% of the same sample are using social media for investigations, then plausibly they are using unofficial practices such as the creation of uncontrolled false personas to conduct these enquiries, suggesting similar activities and practices found in this research are taking place in the US. Finally, while the results considered herein primarily focus on personnel without open source training or social media training, the research captured personnel who have received training in either or both capacity which offers an opportunity to compare practices and knowledge between the two demographics of trained and untrained (See chapter 4.4) which the LexisNexis research could not offer.

Having considered the above population parameters in relation to training, the primary consideration is to evaluate the qualitative commentary from the focus groups together with the qualitative and quantitative survey results to either reject or accept the null-hypothesis. In doing so focus group participants from all three (3) sessions acknowledged anecdotal evidence that open source investigation and intelligence specifically through the use of social media is being conducted by police officers without appropriate training. In each of the focus group sessions participants were asked '*Do police officers use social media for intelligence gathering?*' to which replies included;

Participant: *'We see it all the time, it's very common.'* – Focus Group 1

Participant: *'I know for a fact it happens. You just don't talk about it.'*

– Focus Group 2

While these anecdotal reports suggest the phenomena is taking place, participants were unable to say what, if any training those engaging in these practices had, whether it involved the use of personal social media accounts or false personas or provide confirmation they had witnessed these practices first hand limiting the reliability and validity of the answers elicited. However, focus groups one (1) and three (3) went further by commenting on the practices of their peers and highlighting the impact supervisors played in junior personnel conducting open source research outside of legitimate practices. In those focus groups sessions participants stated;

Facilitator: *'Do you think the organisation understands social media at the higher level ... or do you think they just let people get on with it?'*

Participant: *'I think they let people get on with it.'* – Focus Group 1

Participant: *'I get quite a lot [of requests]. A duty Inspector asked me to hack into a person's Facebook... I don't think they understand. Do they! That's them not understanding. It's been several times; can you check this Facebook account, or can you check this person?'* – Focus Group 3

This issue was also picked up in the qualitative data obtained from the survey results with MPS personnel not only reflecting on requests from their supervisors, but supervisors documenting how they actively request their teams to conduct open source intelligence at level one (1);

Respondent: *'I was asked by a supervisor to look for a suspect on Instagram. As this is an App that one must have a log in to use – I obliged.'* – Survey Question 9

Respondent: *'As a supervisor, I suggest others use it [open source]'* – Survey Question 4

Respondent: *'I direct my team to use it often – Probably around 2/3 times a month.'* - Survey Question 4

The comments made by supervisors demonstrate the issue is not simply one of junior ranks deciding to go against policy and legislation, but an issue of supervisors actively encouraging personnel to engage in such practices. This was also highlighted in LexisNexis (2012, p.3) where their executive summary stated;

'Those in supervisory positions are significantly more likely to use social media for investigations.'

This thematical section considering open source and the front line has shown the key demographics involved are officers of PC/DC rank, aged 35-44, with service of between 10-15 years who have had no training either in the use of open source for investigations and intelligence or social media for the purposes of community engagement. Although unique research, this theme has been compared to the closest available US study which has shown similarities in the key demographics. In addition, it has raised the impact of those in supervisory positions contributing to the phenomenon either by conducting the same practices or directing others to do so. With 78% of personnel without any form of open source training and 77% without any formal social media training the concern should be that this leaves a vacuum for discretionary operational practices to thrive. Discretion becomes pertinent to this theme when there is limited training, operational access and direction for personnel to formulate informed decisions. Cockcroft (2012, p.47) reviews previous work in this area and considers that police culture has tended to highlight the importance of discretion at the lower end of the police ranks. He cites Davis' (1969) definition that 'a police officer may be said to exercise discretion whenever effective limits on their power leave them free to make choices among possible courses of action.' Furthermore, Cockcroft considers Reiss (1974) who believes, 'discretion pertains not only

to the power holder making the decision, but also to the fact that that decision is not subject to review.’ In this instance police personnel will continue using unrestricted access to social media platforms because there is no official oversight to review their actions. However, this issue will not be resolved solely by successful training or an effective infrastructure to facilitate official access to social media platforms, it requires a process that has less systematic friction than taking your personal mobile device out of your pocket and tapping into an application without trace or justification. This would require a cultural shift at all levels of the policing hierarchy and a recognition of the challenges open source presents to policing organisationally. However, the implementation of a new system or process can only be justified with an understanding of what practices are taking place and how frequently they occur in order to determine the benefits of implementation.

4.2.1. Frequency of Open Source Use.

Survey question 4. provides an insight into how often personnel are using open source for investigations by asking, ‘*Approximately how often do you use Online Investigation (Open source) research in your work?*’ with **Table 4.** (see appendix) showing the frequency of use against the number of respondents for each category, with **Figure 8.** (see appendix) showing respondents usage in percentages. This represented the lowest reliability coefficient with a split-half reliability result of $r=0.81$ and represents an area of complexity that would benefit from future research to extract the data with more precision than this survey allowed. However, it does corroborate the comments made in the focus groups where participants stated the existence of surveillance practices. **Table 20.** is filtered to show only level one (1) untrained respondents ($n=685$) together with the frequency each demographic (Grade/Rank) uses online investigation (open source) research in their work (obtained from **Table 4.**). Separated by respondent’s grade/rank the table highlights PC/DCs as the modal category within the demographic utilising open source for investigation purposes either ‘Rarely’, 2-3 times a month ($n=181$) or ‘Occasionally’, 2-3

times a week (n=121). Both categories represent 44% of the responses while PC/DCs represent higher use in all frequencies compared to the other grades and ranks in this demographic.

Table 20. Level 1 Frequency of Open Source Investigation by Grade/Rank

Frequency of Use by Level 1			Grade/Rank						
Level 1 - No OS Training	Frequency	n	Band E	Band D	Band C	PC/DC	PS/DS	Insp/DI	PNTS
Total n=	685								
	V. Frequently (Several Times a day)	49	2	0	0	31	11	2	3
	Frequently (1-2 Times a day)	64	4	1	1	46	8	1	3
	Occasionally (2-3 Times a week)	157	5	0	1	121	22	7	1
	Rarely (2-3 Times a month)	214	3	1	0	181	22	4	3
	V. Rarely (Once a month or less)	138	10	3	0	80	30	10	5
	Never	63	9	0	0	44	9	0	1

n=685, modal response – PC/DC-Rarely,

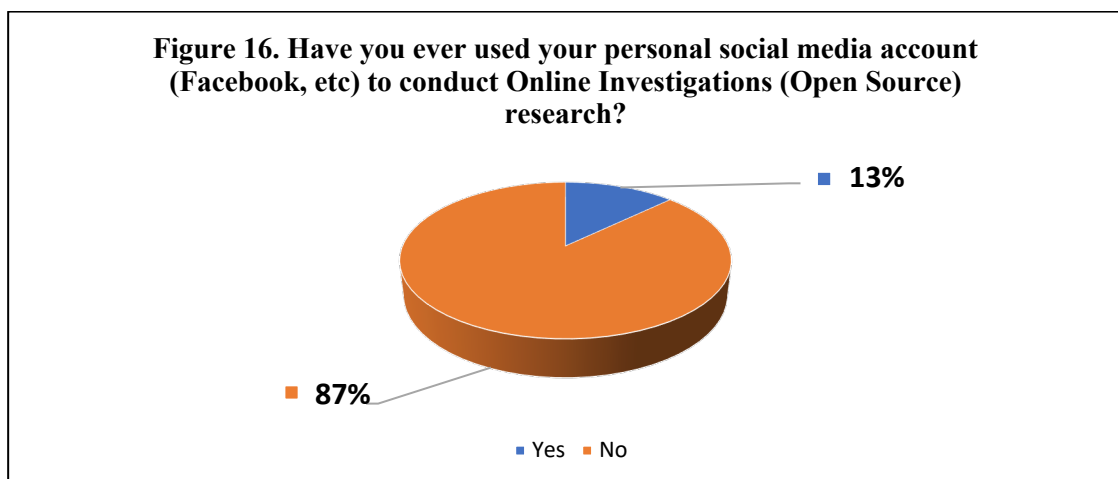
The estimated confidence interval for the population proportion is calculated using the frequency of PC/DCs who indicated they use open source intelligence either ‘Rarely’ and ‘Occasional.’ Therefore, the confidence interval for ‘Rarely’ estimates that the population parameter ranges between N=9,000 and N=11,000 MPS personnel utilising open source two (2) – three (3) times a month. While for ‘Occasionally’ estimates that between N=6,000 and N=8,000 MPS personnel are using open source for investigative reasons between two (2) and three (3) times a week. Although the parameters relate to Level One (1) personnel this in itself does not confirm that they are conducting the open source work themselves. However, it provides an estimate to the number of personnel using open source for investigations in each category. Given that the number of central requests for open source in 2018 was 3,605 (Data obtained from the Central Open Source Unit), the data in **Table 20** suggests that personnel are fulfilling their need for open source elsewhere adding weight to the alternative hypothesis that individuals are conducting the research other than through official channels. **Table 20.** also identifies the phenomenon is not confined to PC/DCs and demonstrates that supervisors, (Band D, PS/DS and Insp/DI’s) also engage in open source investigations, albeit at a lesser frequency.

Frequency of use was considered by LexisNexis (2014, p.4) but was only broken down into four (4) categories of daily (25%), 2-3 times a week (31%), 2-3 times a month (30%)

and less often(12%). While the target audience was only those who use social media on the job comparisons can still be drawn with this research data recording 21% using online investigations daily, 23% used it 2-3 times a week, 16% used it 2-3 times a month, while 31% used it very rarely. However, 9% of this research stated they never used open source for investigations, but it demonstrates the high levels of use internationally and demonstrates that 91% of survey respondents are using social media to some degree for online investigation and research in their work compared to 81% in the LexisNexis study.

4.2.2. Personal Social Media Accounts

The following data sets consider the specific elements of the phenomenon that were articulated by focus group participants and identified in the survey analysis as taking place contrary to MPS policy. The existence of these elements confirms the alternative hypothesis that, social media surveillance is taking place across the service through the use of personal social media accounts and false personas that are accessed primarily via personal devices. **Figure 16.** Shows the breakdown of respondent answers to survey question 9. with n=101 respondents from the sample population stating that they use their personal social media accounts, such as Facebook to conduct online investigations (open source) research. With a sample size of n=785, those using their own accounts represents 13% of participants ($101/785 = 13\%$).



The estimated population proportion uses the percentage of respondent's answers to question 9. to calculate the estimated population parameter for MPS personnel using their personal social media accounts to conduct online investigations. The estimated population parameter for MPS staff using their own social media accounts ranges between **4,000** and **6,000** personnel. The use of any personal social media account for the purposes of intelligence gathering or investigation is not specifically against MPS policy, but it could be argued inappropriate under the current guidance 'using social media for professional reasons' (MPS, 2013, p.5). Here the guidance discusses compromising operational effectiveness but doesn't unambiguously prohibit the use of personal social media accounts for a policing purpose;

'It is expected that you will conduct yourself in such a way as to avoid bringing the MPS into disrepute or compromising its effectiveness or the security or its operations or assets'

The data set contained in **figure 16.** supports the alternative hypothesis that MPS personnel do in fact use personal social media accounts to conduct intelligence research and provides an organisational estimate of the practice. **Table 21.** below takes the analysis of the practice one step further by analysing the distribution of personal social media use across the demographics of age, length of service and band/rank. In doing so it demonstrates the practice occurs across the demographic with modal responses identified for personnel aged between 34-44 years (however, the age range of 25-34 differs by only one (1) respondent) with 10-15 years of service and observes those of PC/DC rank predominantly using their personal social media account for online investigation work.

Table 21. Use of Personal Social Media Account across Age/Service/Rank Demographics

Personal Social Media Account		Age Range		Service		Rank	
Yes Total n=	101	18-24	3	0-2	6	Band E	3
		25-34	33	2-5	18	PC/DC	67
		35-44	34	5-10	18	PS/DS	22
		45-54	23	10-15	24	Insp/DI	5
		55+	2	15-20	17	PNTS	4
		PNTS	6	20-25	8		
				25-30	7		
				30+	3		

While none of the focus group participants openly admitted using their personal social media accounts, survey respondents commented across several survey questions to explain why they used their personal social media accounts. Similar themes resonated through their answers with examples of, *Safeguarding, Investigation and Intelligence Gathering* being presented as the principal reasons (See Appendix H for full analysis);

Respondent: *‘I cannot remember specifically but I have used my private social media accounts to see if mispers have social media accounts and whether there is any useful information.’ – Survey Question 9.*

Respondent: *‘Tracked a Romanian burglar who created a number of profiles. Male had not been arrested before and we could not locate him. Used Facebook to try and discover friend groups the he was associated with and locations of pictures he was uploading’ - Survey Question 7.1.*

The data for this element of the phenomenon evidences that MPS personnel are using personal social media accounts, an activity considered high-risk as the use of a personal account may leave a footprint or trace of the employee’s (officer/staff) search. Not only could this undermine the ‘policing purpose’ for which the search was being conducted but may pose as a potential risk to the individual through the exposure of their personal identity and information. In some respects, the risk is less about accidental ‘liking’ or ‘following’ a potential criminal, and more about the unknown algorithms working in the background. The purpose of social media is to connect people and algorithms in part facilitate those connections by making recommendations based upon who has visited a

profile, page or put a mobile number into their phone. This concern was captured by a survey respondent when asked if they had used their personal account;

***Respondent:** 'No as there can be a trace which would link my personal account to having searched for the suspect and Facebook may then use that data to link me to the subject. He would then be able to find me despite the use of high security settings.'* – Survey Question 9.

While Trottier (2014, p.82-83) is correct when he states, 'we may think of police surveillance on social media as one single process, yet there are several categories' with the first category detailing manual searches by investigators and identifying that these practices are taking place by ground-level personnel. However, it assumes that those practices are being conducted through appropriate, authorised channels by trained individuals with a top-down mandate providing effective oversight to safeguard against inappropriate practices. While Trottier's first category is correct and those individual appropriate enquiries do take place, this research suggests a seventh category below his current six, where unofficial police use of social media creates surveillance practices that are rationalised by practitioners as 'for a policing purpose.'

4.2.3. False Personas

A false persona is a fake social media profile and is strictly governed within the MPS with only trained open source personnel of level two (2) – five (5) allowed to create and maintain them. They are recognised by ACPO (2013, p.7) as necessary to gather online information from platforms such as Facebook and Twitter. Accessing these platforms covertly requires an account in order to carry out observations of another user or group. The only purpose in using a false persona is to act covertly in those observations. While the creation of a false persona does not require authorisation under RIPA, all false personas must be authorised, and a record maintained by a Detective Inspector in Intelligence or Covert Policing. The use of false personas was discussed during each focus

group session and while none of the participants detailed any instances of either themselves or others using them it was evident that there was confusion over what a false persona was or how they could be used;

Facilitator: *'How do you feel about false personas?'*

Participant: *'I think you would need some authority to do that.'* – Focus Group 1

Facilitator: *'Level 2 and above allows you to adopt a false persona, at level 3 you can befriend and eventually at level 5 you can engage in conversation.'*

Participant: *'Does that mean if you are using Met Twitter and you follow @plumstead? People talk on there ... would that be?'*

Facilitator: *'Not quite, you are using a Met account and are completely Overt.'*

– Focus Group 2

In focus group three (3) participants intuitively raised the issue of false personas and discussed how their use may impact public trust;

Participant: *'I think we are going to lose a lot of trust by being able to interrogate anyone's social media account. We need to have some boundaries ... to keep public confidence.'* – Focus Group 3

Although survey question 10. asked respondents if they had used a false persona to conduct online investigations, it did not provide the opportunity to add comments. However, respondents provided valuable commentary throughout the survey in relation to their use of fake accounts and false persona;

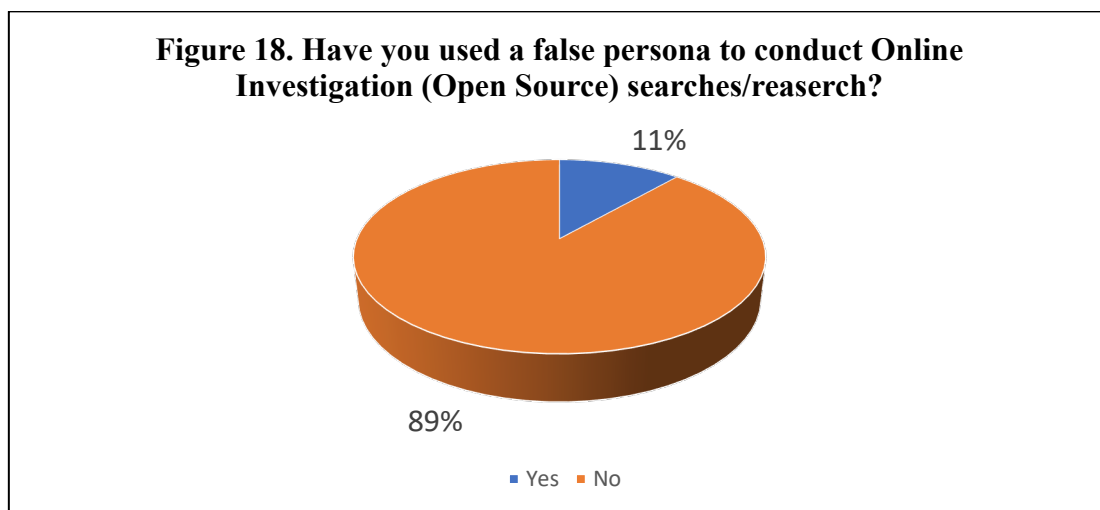
Respondent: *'I have a fake account that I use for work just like many other investigators have.'* – Survey Question 9.

Respondent: *'Normally around locating high risk mispers or high-risk suspects. I work on response team and this is when no one is available with an approved Facebook account. This is when the research is time critical. I know I should not but for the sake of expediency I have created a Facebook account solely for this purpose.'* – Survey Question 5

Respondent: *'I maintain a simple dummy account to use for research. I am aware that I cannot interact with other account users.'* – Survey Question 9.

The qualitative data demonstrates the ease with which a false persona can be created and remain covert not just from the public but from internal monitoring, auditing and authorisation. As the society increases its use of these platforms so will the need and desire for the police to access the data and with the relative intangibility that data surveillance brings, there will be no physical exposure to authority (McMullen, 2015) meaning that the public will be unaware of any surveillance activity they become observed in.

Figure 18. represents the percentage of respondents for survey question 10. who stated they had created a false persona for online investigations, with 11% or n=90 respondents across the sample and filtered to include only personnel at Level One (1). This provided an accurate statistic for those using false personas against policy and without authorisation.



The validity of this question raised consideration around knowledge levels of what a false persona meant. However, this was not considered an issue in survey pre-testing, the term 'false persona' is widely used throughout the MPS and the survey targeted professionals within the policing environment. The use of 'false personas' filtered by Level One (1) personnel represents n=24 or 3.5% of respondents (24/685) within the survey data.

Calculating the estimated population proportion produces a range of between **800** and **2,000** personnel who are utilising false personas to conduct online investigation (open source), research. Again, this supports the alternative hypothesis that social media is being used for surveillance purposes and rejects the null hypothesis. **Table 22.** Takes the analysis further to represent the respondents (n=24) by their age, length of service and rank highlighting the modal responses for respondents as aged between 34-44, with 10-15 years' service and of PC/DC rank.

Table 22. Level 1 use of a False Persona across Age/ Service/Rank Demographics

OS Level 1 using a False Persona		Age Range		Service		Rank	
Level 1 n=	24	25-34	4	2-5	1	PC/DC	17
		35-44	13	5-10	4	PS/DS	4
		45-55	7	10-15	10	Insp/DI	2
				15-20	2	PNTS	1
				20-25	6		
				25-30	0		
				30+	1		

While there is no comparative research to compare this analysis against the use of a false or fake accounts was raised by Mateescu, *et al* (2015, p.5) who has concerns over the violation that these accounts represent to public rights arguing that they represent a cheap and disproportionate method of conducting surveillance on the public. In contrast they articulate how the creation of these accounts, whether authorised or not is a violation of the terms of service for many social media platforms who ban law enforcement creating fake identities. Although a relatively low statistic this finding has the worrying potential of becoming more prevalent in time, with LexisNexis (2014, p.4) recording that 43% of respondents stated they believed a significant increase in the use of social media for investigations was likely. The embedding of these practices as 'accepted' arguably represents a bottom-up manifestation of state power in the form of law and order politics that includes profiling, discrimination (Trottier, 2012, p.75) and directed targeting through localised surveillance. The key issue with the use of technology for these purposes is that unchecked surveillance creep can have a significant impact on police legitimacy and how the public view their personal data being used fairly, appropriately and transparently. The

use of unauthorised false personas offers no reassurances against abuse of power, and goes against the principles of legitimacy, especially without the oversight to ensure consistent proportionality and necessity in their application. Bottoms and Tankebe (2012, p.124) recognise the power dynamic intrinsic to policing and raise the question of legitimacy in terms of, ‘whether the power-holder is justified in claiming the right to hold power over citizens.’ The purpose of policies and legislation is to ensure that the exercise of power is appropriate for the purposes in which it is being applied but this cannot happen if the activities taking place within the organisation are covert and unauthorised. Consideration must be given to the methods by which police personnel are actively engaging these platforms in the course of their duties.

4.2.4. Personal Devices

The last element to the phenomenon that is central to its occurrence is the presence and accessibility of personal mobile devices with access to the internet which all focus groups raised and discussed during their sessions;

***Participant:** ‘I think a lot of us are aware that we are not supposed to use our phones for this kind of research no matter how good our intentions are.’ –Focus Group 1*

***Participant:** ‘The problem is that people are doing it on their mobile phones, there is no record of what they we’re doing? People certainly aren’t putting on any crime reports or criminal intelligence reports to say they are doing checks.’ –Focus Group 1*

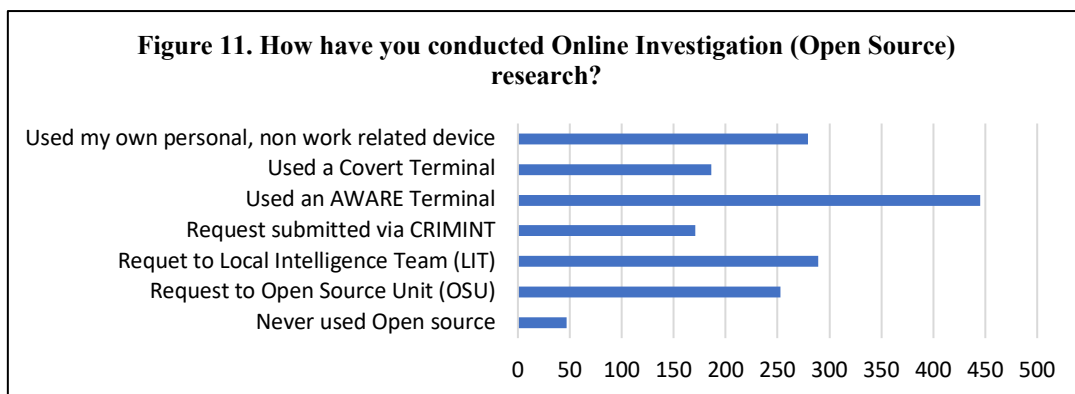
In survey question 7. respondents were asked, ‘How have you conducted online investigation (open source) research?’ with **Table 6.** showing the frequency of the various methods available to MPS personnel. The question allowed respondents to select more than one option giving a total response of n=1670 with the modal response being, ‘Used

an aware terminal’ (n=445) but of particular interest is the frequency of respondents who used their own personal, non-work-related device (n=279) to conduct online investigation (open source) research. This represents 36% (279/785) of respondents who have used their personal devices. The horizontal bar chart in **Figure 11**, provides a clearer representation of the various methods used by respondents and articulates that the phenomenon is not an ‘either/or’ scenario with respondents using official channels in addition to their own mobile devices interchangeably to conduct open source work.

Table 6. Frequency of methods used to conduct open source research.

How was Research Conducted?	Frequency
Used my own personal, non-work-related device	279
Used a Covert Terminal	186
Used an AWARE Terminal	445
Request submitted via CRIMINT	171
Request to Local Intelligence Team (LIT)	289
Request to Open Source Unit (OSU)	253
Other (Never used open source)	47

n=785 Respondents, n=1670(no. of answers), modal response Used an AWARE Terminal (445).



The population proportion estimates a range of between **13,000** and **15,000** MPS personnel are using their personal devices for the purposes of open source investigations. This is not particularly surprising as it was identified by the London Assembly in ‘Smart Policing’ (2013, p.10) and while they were addressing the use of ICT generally rather than the use of open source their comments are still pertinent. They stated;

'1.12 The Met also faces challenges in regaining operational advantage over criminals. Criminals using commonly available smartphones may have better technology than officers, as demonstrated by the 2011 riots. Currently, a parallel ICT infrastructure is in place at the Met: police officers use their personal smartphones since these can be more effective at helping them do their jobs than the kit provided to them.'

Although they do not make a direct connection between the use of personal smart phones and the surveillance tactics the statement goes some way to demonstrating the systemic complacency of the capability of these devices by policing practitioners. However, accessing open source intelligence via a personal device, such as a mobile phone is a clear violation of MPS policy (2014c, p.2) which states,

*'Investigation or research over the internet **must not** be carried out on personal devices. This activity can pose a risk to the personal safety of the individual and/or that of their family and may also compromise operational activity.'*

As stated, using a personal device for the purposes open source investigation applies to all MPS personnel regardless to the level of open source training, therefore **Table 23**. Correlates the results to the survey question, *'How have you conducted online investigation (open source) research'* and specifically the option, *'Used my personal, non-work-related device (your own phone/tablet etc)'* against the demographics of level of open source training, age, length of service and grade/rank.

Table 23. Use of personal device to conduct online investigation (open source) research across Open Source Training/Age/Service/Rank Demographics

Yes' to using personal device n=279							
OS Training	Age Range		Service		Rank		
Level 1	257	18-24	6	0-2	16	Band E	11
Level 2	19	25-34	91	2-5	52	Band D	1
Level 3	3	35-44	101	5-10	54	Dand C	2
Level 4	0	45-55	60	10-15	74	PC/DC	198
Level 5	0	55+	6	15-20	51	PS/DS	50
		PNTS	15	20-25	16	Insp/DI	11
				25-30	13	PNTS	6
				30+	3		

The results show that while the modal response is level one (1) trained personnel (n=257), the phenomena also takes place by those trained at level two (2) and three (3) indicating that the use of personal devices is not completely removed by training, particularly at level (2). The modal responses across the survey sample are those aged 34-44 (n=101), with 10-15 years' service (n=74) and of PC/DC (n=198) rank. Several risks arise from the use of a personal device for official intelligence gathering and investigational work, firstly the prospect of releasing personal data, including the devices IP address to those the practitioner is conducting surveillance work on exposing themselves and any operational activity they are conducting. Secondly, as detailed by Sampson, (2017, p.65) there is a core issue with the admissibility of OSINT material obtained by the police that relates to the means by which it was obtained with the definition and parameters of what amounts to 'unlawfully' obtained material often in legal dispute. Issues have arisen many times in relation to potential breaches of Article 8 of the ECHR which allows for the materials admissibility to be challenged in court. As Sampson articulates the key element is the fair administration of justice which in the view of the European Court of Human Rights, 'holds so prominent place in a democratic society ... it cannot be sacrificed for the sake of expedience.'

In summary the survey data in this theme supports the alternative hypothesis and describes how MPS personnel are conducting open source intelligence and investigations using social media and while it is predominantly PC/DC's engaging in these practices, there is representation across the demographic of police officers and staff, only to a lesser extent. The survey data observes respondents aged 25-44, with 10-15 years' service of the rank of PC/DC use their personal social media accounts, false personas and personal devices to carry out intelligence work across social media platforms which suggests key demographics to target in order to have the most significant reductions in these practices.

The inference of the survey results has been estimated against the true MPS population proportion and while based on statistical survey data, it is recognised that because the number of untrained personnel at level one (1) is likely to be higher than represented in the survey there will be an impact on those inferences. It is argued that because the number of personnel at level one (1) represented in the survey (n=87%) is lower than the estimated population proportion of N=98% the analysis can infer that the parameters observed in the sample represent at best, the lower range of expected values in the population. **Table 24.** summarises the statistical findings of this chapter and helps to summarise the concerns raised throughout this chapter in relation to the use of localised surveillance tactics by policing personnel. As concluded in Sampson (2017, p.66) while there is a responsibility to consider the provenance and reliability of social media intelligence, there is also a need for law enforcement agencies to consider how they came by the material and what processes they used to obtain it and that failure to consider these issues at an early stage may prove fatal to a prosecution or related proceeding.

Table 24. Ch. 4.2 Summary of key findings and inferences against MPS Population.

Theme	Survey Response (n)	Percentage (%)	Estimated Population Proportion (N)
No Open Source Training	685/785	87%	30,000 to 39,000
No Social Media Training	606/785	77%	29,000 to 31,000
Level 1. Use of Personal Social Media Account	101/785	13%	4,000 to 6,000
Level 1. Use of False Persona	24/785	3.1%	800 to 2,000
Use of Personal Device	279/785	35.5%	13,000 to 15,000

4.3. Open Source in a Policing Context

Having established the occurrence of the alternative hypothesis, the null hypothesis can be rejected opening the next phase of analysis which considers what police personnel are using OSINT and SOCMINT for and why they are going against policy and legislation to access these data streams for policing purposes. A number of themes were established

from the data including the dichotomy between justifying the use of using open source for matters of safeguarding opposed to investigations and intelligence gathering. However, at a fundamental and practical level, justification was articulated in terms of basic policing needs; the need for real time information at the scene while still relevant; the need for technology to enable personnel to conduct open source research quickly, safely and efficiently and finally a need to feel empowered to conduct investigations using capable technology fit for purpose and representative of modern policing.

4.3.1. Safeguarding Vs Investigation & Intelligence

Throughout the three (3) focus group sessions participants attempted to explain why ‘their peers’ were using social media under the principle of ‘for a policing purpose.’ On the hand they could understand and justify its use in terms of protecting the vulnerable, mitigating risk and the belief that necessity outweighed any breach of policy. This was often framed in examples by participants referring to locating and safeguarding of high-risk missing persons;

***Facilitator:** ‘Do you feel that if it’s a vulnerability issue [rather than an investigation] the means justify the ends in terms of looking at open source?’*

***Participant:** ‘Yeah, you would often go to your Local Intelligence Team (LIT) team for this, but if it’s Sunday night and no one is in, what else are you going to do. If you don’t know there is 24/7 support, you are going to look it up yourself.’ – Focus Group 2*

In contrast participants articulated the use of social media to trace suspects or follow individuals of police interest in less favourable terms;

***Participant:** It’s about risk, its immediacy and proportionality. Is it worth checking [social media] to see where you checked in over the last two (2) weeks because you are a shoplifter? No, however, you are a regular missing person, you’re a child and you constantly go missing at the weekend and I can see that you are at the same nightclub for the past five weekends ... 99% of the public would support that.’ – Focus Group 3*

The propensity for participants to justify policing practices in terms of safeguarding and risk management while being less empathetic towards its use for monitoring, investigation and suspect identification/location suggests the presence of evaluation apprehension (Fern, 2001, pp.106-107). Where participants felt more comfortable presenting the use of social media as a surveillance tool in a positive, altruistic light rather than constructing the phenomena in terms of ‘Big Brother’ watching the public. In doing so participants were able to find a common ground that presented themselves in a favourable light to each other. However, while the focus groups articulated the acceptability of social media in the use of safeguarding, survey respondents answering the questions independently were more receptive to the idea of using platforms for intelligence and investigations. In survey question five (5), respondents were asked to, ‘*Briefly describe how you use/have used online investigation (open source) research?*’ Filtering the results of question five (5) by Level One (1) trained personnel (Full analysis in Appendix H) produced **Table 25**. which represents a word frequency query performed through NVIVO and identifies three (3) themes from the survey respondent’s descriptions of how they used open source research in their work:

**Table 25. Word Frequency for Question 5.
Briefly describe how you use/have used online Investigation**

Key Words Searched	Themes	Frequency
Intelligence, intel, intels, research, researching, researched, search, searched, searching, researchers, searches, information, inform, informant	Intelligence Gathering	237
Suspect, suspected, suspects, investigate, investigation(s), investigating, investigative	Investigation and Suspect Identification/Location	200
Missing, missed, misper(s)	Safeguarding	71

In contrast with the focus groups, safeguarding ranked third on the reasons why personnel used online investigations, with intelligence gathering and investigations scoring higher in the word frequency count. *Intelligence gathering* represented the most common theme in the analysis with variations including ‘*intelligence*’, ‘*research*’ and ‘*information*’ all

referring to the collection and use of data for a policing purpose. The theme was referenced 237 times and represented a weighting of 5.11% across the analysis. In London Assembly (2013, p.27) it was recognised that social media was a useful source of intelligence and stated that the Met was starting to use tools to monitor protests and events planned on the internet. However, the examples presented by respondents demonstrate that intelligence gathering while diverse is taking place on a more localised scale than that suggested by the London Assembly with a variety of examples being provided;

Respondent 1: *'Open source on social media provides valuable intelligence on subjects under investigation so at every opportunity social media is checked for latest photos, personal information on whereabouts both past and current. This can be used obtain information which can then allow police to apply for further [court] applications.'* – Survey Question 5.

Respondent 2: *'I regularly search the internet and social media for Intel and Info purposes to help and assist with events planning. Although we have a Local Intelligence Team, they are often busy with other requests and mainly deal with crimes rather than public order.'* – Survey Question 5.

The key word '*suspect*' and its derivatives represented the most frequently used term within the analysis, referred to n=133 times and was closely linked to the term '*investigation*' and its associated derivatives. There is a logical connection as investigations tend to seek a suspect responsible for the allegation being investigated. Together the two (2) terms had a combined weighting of 4.76% over the entire text and supported the initial findings from the focus groups that open source and social media are utilised for *investigative* purposes for example;

Respondent: *'Used in investigations, to trace suspects, to establish if victims had contact with the suspect.'* – Survey Question 5.

The final theme, *safeguarding* was chiefly contextualised in the data by respondents using social media to locate or find information on missing persons as in the focus groups. The

key words identified were 'missing' and 'misper' (a term used within the MPS to refer to 'Missing Persons') that resulted in the inclusion of this theme with 71 references being made within question five (5) and a weighting of 1.21%. A search of associated words such as, safe, safeguard and vulnerable yielded no additional results. Comparing the weightings of the three (3) themes shows statistically that safeguarding was not as important to the survey respondents as it was to the participants of the focus group but still featured.

***Respondent:** 'Whilst working on the misper unit - open source research, for example Facebook was a great tool for monitoring some of the mispers who were out of 'contact' but would post on social media so we could establish that there were alive and seemingly well.'* – Survey Question 5.

Perhaps unsurprisingly the analysis recognised the overlap between the three (3) themes where intelligence gathering can relate to either an investigation and/or a matter of safeguarding but warranted its own theme due to the variety of functions that the police are employed to carry out within society and require the development of intelligence to make effective decisions on (e.g. public order events). The qualitative analysis of question five (5) does, however, demonstrate the breadth of uses open source data and social media has in a policing context and is visually represented in the below word cloud. **Figure 29.** shows the top 60 words identified in the NVIVO frequency analysis of survey question five (5) and provides a context around the key words that drove the development of the above themes.

The saturation of social media is a result of its domestication, that is the degree to which it has been embedded in everyday life (Trottier, 2012, p.78) and so it is not surprising it has migrated from personal use to police use at the localised level. Police personnel use these platforms personally and identify with the benefits professionally. However, as

devices to access open source for the purposes of investigation and intelligence the qualitative commentary explored the reasons for use of personal devices, with one (1) focus group participant stating;

Participant: *'[using your personal device for intelligence gathering] It does happen regularly. We see it all the time, it's very common and whether on YouTube or Facebook you seek the suspect. I mean it's very common.'*

- Focus Group 1.

These comments are supported by the qualitative commentary obtained from question 7.1. which highlights the key types of work being carried on personal devices as investigative, safeguarding and intelligence based;

Respondent: *'Trawling social media quickly reacting to information from a victim to determine if the information was accurate and would lead to a potential suspect being identified. Once confirmed that the information was accurate, I then submitted an official request to have the social media account evidentially captured.'* – Survey Question 7.1.

Respondent: *'I have used my personal mobile and tablet to see Facebook profiles and gain info from the press. It is the quickest way of seeing the information that is in the public domain.'* – Survey Question 7.1.

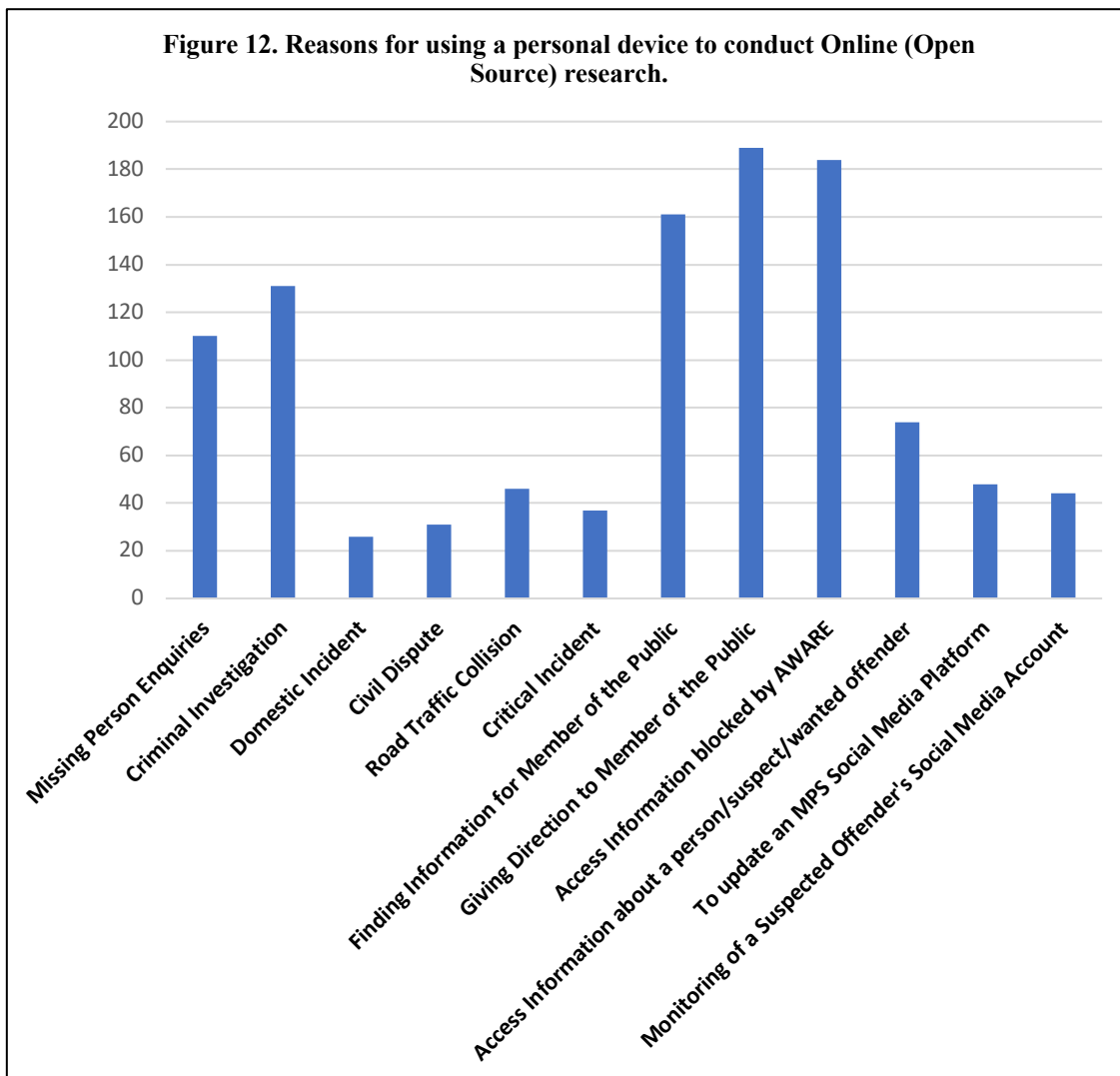
The majority of comments detail research being carried out for the purposes of conducting investigations, with safeguarding second and intelligence gathering rarely mentioned, suggesting that personnel are using mobile devices predominantly to access information immediately to assist with ongoing police matters, rather than for protracted monitoring of intelligence.

Survey question 7.1. takes the responses to question 7. of those who stated that they use their personal mobile devices to conduct open source research (n=279) and asks them to detail what they use their personal devices for. **Table 7.** shows the breakdown of responses

across this multiple selection question, with n=1084 representing the total number of answers by the n=279 respondents. The bar chart in **Figure 12.** shows the frequency of those responses and identifies the modal response as being the provision of directions to the public which is considered an appropriate use of the technology. However, respondents also use their personal device for safeguarding with n=110 conducting missing person enquiries, and while criminal investigation represented n=131 responses, as a theme criminal investigation could include the categories, Domestic Incident, Civil Dispute, Road Traffic Collision and Critical Incident as they are types of investigations. To avoid double counting only independent responses across each theme have been included to establish an estimated confidence interval for thematical analysis. (Note: If a respondent ticked yes to more than one answer within the theme it has only been counted once within the thematical context). Therefore, the combined categories that represent the theme of investigation total n=167 (n=131+3+8+20+5). Responses involving intelligence gathering either by accessing information about persons/suspected/wanted offenders or monitoring a suspect's social media account equal n=66 (n=33+33).

Table 7. Reasons for using your Personal Device

Reason for Using Personal Device	Frequency	Thematical Value
Missing person enquiries	110	110 (Safeguarding)
Criminal investigation	131	131 (Investigation)
Domestic Incident	26	3 (investigation)
Civil Dispute	31	8 (Investigation)
Road Traffic Collision	46	20 (Investigation)
Critical Incident	37	5 (Investigation)
Finding information for member of the public	161	161
Giving directions to members of the public	189	189
Accessing information about a person/suspect/wanted offender	74	33 (Intelligence)
Access Information blocked by AWARE	184	184
To update an MPS social media platform	48	48
Monitoring of a suspected offender's social media account	44	33 (Intelligence)



n=279 Respondents, n=1084(no. of answers), modal response – Giving Directions (189).

It was previously established in chapter 4.2.4 that the number of personnel using a personal device for open source research was n=279 and represented an estimated N=13,000 and 15,000 across the population size. Utilising the three key themes identified it is estimated that the population proportion of MPS personnel using personal devices for purpose of *investigations* is between 8,000 and 9,000. The number of personnel across the MPS using their personal mobile devices for the purpose of *intelligence gathering* is between 3,000 and 4,000. Finally, the number of personnel across the MPS using their personal mobile devices for the purpose of *safeguarding* is between 5,000 and 6,000.

Based on the above data it suggests personnel are utilising their mobile devices predominantly for the purpose of *investigations*, then *safeguarding* and finally *intelligence gathering*. It is recognised that the question simplifies the complex nature of police activities and that validity of the thematical analysis may be impacted on the loose inclusion of answers into themes that were not specified at the time of asking the survey question. This represents another area for further research but provides a loose interpretation of the data to compare against the word frequency analysis in chapter 4.3.1. There the data suggested the order of significance for MPS personnel carrying out online research was *intelligence gathering*, *investigation* and then *safeguarding*. As such the quantitative data could suggest personnel are conducting real time open source research during potentially live investigations and matters of safeguarding, while intelligence checks may be a less time sensitive and therefore not requiring the use of a personal device as often. If this were the case the qualitative responses don't support the quantitative reasons provided.

While there are no comparative studies to compare these finding, **Table 7**. Confirms surveillance activities as a minimum are taking place with the n=44 respondents using social media to monitor suspected offenders accounts which represents a total of 5.6% of the overall survey (n=44/785) results and suggests an estimated population proportion of between **2,000** and **3,000** MPS personnel. These respondents also stated they were level one (1) untrained personnel. This activity contradicts the guidance on 'repeated viewing' of personal information and constitutes directed surveillance under the *Regulation of Investigatory Powers Act 2000*. Without the correct authority it is highly likely that it constitutes breaches under the *Human Rights Act 1998*, article 8, the right to a private and family life and contravenes MPS policy and codes of conduct. As highlighted earlier in these findings, practices that fail to be conducted with proportionality or necessity

severely impact public perception and approval (Clapham, 2015, p.110) and ultimately undermine the confidence the public hold in the police. If the police are to use these tactics they must do so with proportionality, necessity and transparency and only employ them for a legitimate aim. In the case of localised surveillance these important concepts distinguish the police and the rule of law from the rest of society are absent and serve only to diminish the evolving dialogue between the power holders (police/state) and audiences (the public) that maintains the legitimacy of the police as rightful power holders (Bottoms and Tankebe, 2012, p.120).

4.3.3. Why Personnel don't use the Open Source Unit

In the previous chapters it was identified that MPS personnel are using their own devices to conduct investigations, manage matters of safeguarding and obtain intelligence with these themes being represented through the paradigm of a 'policing purpose' to justify the means by which information is obtained. To facilitate these enquiries, personnel are using false personas and personal social media accounts in contradiction to MPS policy and guidance specifically around the 'repeated viewing' and the use of personal devices, while at the same time potentially breaching legislation. This chapter will explore 'why' personnel are putting themselves in this position by utilising the quantitative data obtained from survey questions six (6) and eight (8) and the qualitative data obtained not only through the focus group sessions but throughout the survey. Survey question 6. asked respondents whether they are aware of the Internet Intelligence and Investigation (i3) Team (Open Source Unit) who can support them with open source research. **Table 5.** (See appendix) shows the frequency of respondents who are aware of the i3 Team with **Figure 10.** (See appendix) representing the percentage of respondents aware of the i3 Team and exhibits that 52% of respondents stated they are unaware of the support available to them in conducting open source research through the central team.

This suggests an estimated population proportion between **19,000** and **22,000** MPS personnel are unaware of the i3 (Open Source) Team or that they can assist with open source research on their behalf. While 52% of the sample didn't know the i3 (Open Source) Team existed there are other reasons that resonated throughout the research as to why MPS personnel chose to conduct open source research independently of the support offered by both their Local Intelligence Teams (LITs) and the i3 (Open Source) Team. The qualitative data from focus group sessions and the survey identified the following themes to explain why MPS personnel used their own personal devices;

Efficiency

Its Open Source

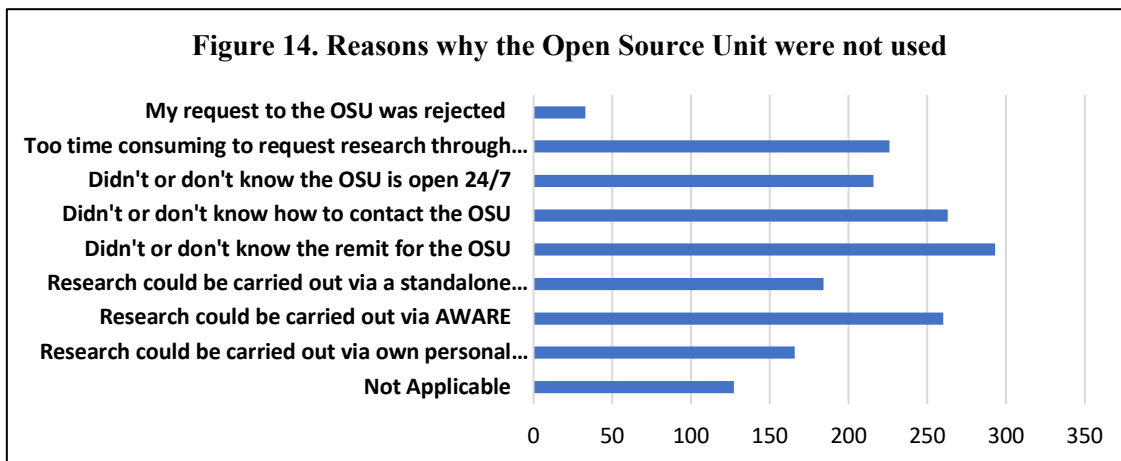
Self-Service

Restrictive IT Systems

In support of these themes survey question 8. asked respondents, '*Are there any specific occasions/reasons for why you have not used the services of the Open Source Unit?*' with **Table 8.** representing all n=1768 answers from the n=785 respondents and the modal response stating that respondents didn't know the remit of the open source unit.

Table 8. Reasons why the Open Source Unit (OSU) were not used

Reasons why Open Source Unit (OSU) were not used	Frequency
My request to the OSU was rejected	33
Too time consuming to request research through the OSU	226
Research could be carried out via own personal device	166
Research could be carried out via AWARE	260
Research could be carried out via a standalone (Inc. LIT or colleague)	184
Didn't or don't know the remit for the OSU	293
Didn't or don't know how to contact the OSU	263
Didn't or don't know that the OSU is open 24/7	216
Not Applicable	127



n=785 (no. of Respondents) n=1768 (no. of answers), modal response – Didn't know remit of OSU (239).

4.3.3.1 Efficiency:

With the advent of mobile phone technology and social media applications everyone has ready access to the internet through their phone or variety of mobile digital devices. This creates a situation where MPS personnel have an efficient means to access information in the palm of their hands. It is therefore difficult to establish organisational practises that are faster or less system friction. This was articulated across all focus group sessions with respondents stating the benefits of using their own devices;

Participant: *[Referring to social media engagement] 'I've tried using the work phone, it's pointless!'*

Facilitator: *'And so you revert back to your own phones?'*

Participant 1: *'Oh god yeah. We just revert back to whatever is easy generally with all things.'*

Participant 2: *'It's easier just to use your own phone, you own minutes.*

I mean we all get free minutes now anyway, so it doesn't cost me anything to use my own phone.' Focus Group 2

It was also identified in the survey data that respondents felt placing a request for open source work to be conducted was an inefficient process when they needed the information immediately and adds weight to previous conclusions around the need for investigational and safeguarding information quickly;

Respondent: *'Not operationally effective to continually make requests, information required at that point.'* – Survey Question 8.

Respondent: *'It's easier than having to go through the Open Source Unit – Fast time intelligence is required and do not have to fill in a form.'* – Survey Question 9.

Respondent: *'It is the 21st century. Why would I waste time making a request when I can do it on my phone which is in my pocket. Unless I needed it in an evidential format and for a paper trail for legal reasons there is no way I would bother making an official request. Unless I had been given the training to do it myself.'* – Survey Question 7.1.

Figure 13. (See appendix) confirms these qualitative comments exhibiting that n=226 respondents stated that 'It was too time consuming to request research through the Open Source Unit' and n=166 respondents stated that 'The research could be carried out via their personal device' representing 29% and 21% of the sample size respectively. The confidence interval for respondents who stated using i3 (Open Source) Team was too time consuming is:

The true range for the population proportion of the MPS is therefore between **10,000** and **13,000** who believe that it is too time consuming to use the i3 (Open Source) Team. In relation to the respondents who stated that they could use their own device to carry open source research the confidence interval is:

The true range for the population proportion of the MPS is therefore between **5,000** and **7,000** who state they can do the research via their personal device. If the MPS is to reduce practices of localised surveillance it needs to ensure that its staff are aware of the support available to them and constantly work towards streamlining processes to make official routes to accessing OSINT and SOCMINT more attractive to personnel.

4.3.3.2 Restrictive IT Systems:

In correlation with the fact that MPS personnel felt it easier to use their personal devices to conduct official investigative and intelligence research; is the issue of restrictive access to the internet through the MPS IT system AWARE. However, in slight contradiction n=260 respondents to question 8. stated that using the internal MPS AWARE system was a reason not to need the support of open source research through the i3 (Open Source) Team, yet the restrictiveness of MPS IT also featured heavily in respondent answers to question 7.1. as the main reason (n=34 comments) why they use their personal devices with focus groups making similar comments;

Participant: *'You could argue that the MPS is trying to say, "You can't do this" because they block sites like YouTube and certain aspects of Twitter. But it is not clear for u, we are investigators and if one avenue is blocked, we will find another one [Group Agrees]. I can't access it on Firefox, my phone will do it.'*

Facilitator: *'Do you think this is something that happens regularly?'*

Participant: *'Oh yeah' [Multiple participants make agreeing sounds]*

– Focus Group 2

Participant: *[Using social media for intelligence purposes] 'It happens all the times and is always done on their own phones because their access to AWARE is restricted.'* *– Focus Group 1*

While survey respondents agreed declaring;

Respondent: *'It's happens multiple times as the aware terminals are quite restricted, the stand-alone terminals are few and far between (or hidden in a proactive team office), it is usually the quickest and easiest way to carry out the task at hand.'* *– Survey Question 7.1.*

Respondent: *'Websites frequently blocked on Aware, most recent example being a YouTube video linked to a gang-related murder that could not be*

viewed on Aware. Everyone on the MIT team had to view the video on their personal phone. Google Maps is unusable on Aware via Firefox.'

– Survey Question 7.1.

4.3.3.3 It's Open Source

Throughout the focus groups an underlying assumption began to develop about the information personnel were trying to obtain from the internet. Specifically, that because it was considered 'open source' it was 'fair game' for any policing purposes. In one focus group a participant articulated this as;

Participant: *'It should be down to the fact that it is in a public profile, that it's an open public profile. Then I can see any major issue because it's out there anyway. I can see any issue of going to someone's Facebook account because we have done it before. It's an open profile, there is nothing stopping anybody looking at it.'* – Focus Group 1.

While qualitative comments from survey respondents were used to contextualise and justify why they used their personal devices;

Respondent: *'I have used my personal mobile and tablet to see Facebook profiles and gain info from the press. It is the quickest way of seeing information that is in the public domain.'* – Survey Question 7.1.

Respondent: *'The fact that it's open source means it is easily accessible.'*

– Survey Question 8.

4.3.3.4 Self Service

In many instances police personnel are left to get on with the job at hand and while there is support available, personnel tend to be self-reliant and self-driven with the desire to move each job along. In a policing context the next investigation or job is just around the corner which only breeds frustration when the task at hand can be self-fulfilled. In this respect the belief in MPS personnel that they can complete open source research themselves without the need to involve the Local Intelligence Teams (LITs) or the i3

(Open Source) Team ran through the qualitative analysis. While ‘necessity’ formed part of this rhetoric the underlying belief was, ‘I can do this myself’ as evidenced by the focus groups;

Participant: *‘You know we are all adults! If we can’t do something one way, we’ll find another. We won’t go back to mommy and say this isn’t working, give me access. It’s time consuming, I wouldn’t even know who to get in touch with for the whole Web-Marshall thing. I’d just ignore it, when I see that page, I close it and just go to the phone because it’s there.’ – Focus Group 2*

Respondent: *‘As OIC I would rather do the work myself and be assured it’s to a high standard.’ – Survey Question 8.*

Respondent: *‘Every person (nearly) has access to a smart device with internet access. It is ridiculous to not use a tool that has access to a wealth of all human knowledge that sits in the palm of your hand. It would be preferable not to use my own device (due to personal costs to have it and access services) but it is foolish not to use something that would aid in your day to day work/life.’ – Survey Question 7.1.*

Respondent: *‘I have a fake account that I use as it is the only way to get the job done without filling in a load of forms’ – Survey Question 9.*

Table 26. summarises the key quantitative finds from this chapter which has shown a combination of reasons presented by MPS personnel to justify why they resort to the use of their personal devices and accessing sites either through their personal social media accounts or through false personas. With respondents qualifying the identified practices by describing the desire to support victims and investigate crimes at one end of the spectrum, while at the other to support the vulnerable, find missing people and ensure safety. These reasons suggest an underlying desire to make the job work and emanate from a belief that as police personnel, they are engaging in these practices for altruistic purposes, therefore justifying the means. However, the presence of this rhetoric

demonstrates in some respects the failures of recent reports to make technology and access to it the priority promised (London Assembly; 2013; HMIC, 2015) and illustrates a lack of understanding on the part of the agencies and departments generating these reports, as not one mentions access to open source research for frontline policing practitioners. In the reviews and recommendations that this research identified over the two years of research, all highlighted the importance of social media, but it was identified as either an intelligence tool suitable from an organisational point of view to collect masses of data, or as an important engagement tool to be used for intelligence gathering through the open engagement and communication with online communities. The provision of skills and training in this area have been siloed into centralised specialist roles within the MPS making official access to open source data sets time consuming and bureaucratic and resulting in the unofficial practices described. The MPS needs to consider how it can decentralise some of the basic OSINT and SOCMINT enquiries and support frontline staff perform the research they need to effectively and efficiently perform their roles. However, what begins to emanate from the commentary is the lack of awareness that MPS personnel have in relation to their representation of the state, of policing and that they are bound by policy guidance and legislation that not only protects them but protects the public from intrusions into their privacy too.

Table 26. Ch. 4.3 Summary of key findings and estimated inferences against MPS Population.

Theme	Survey Response (n)	Percentage (%)	Estimated Population Proportion (N)
Use of mobile device for the purpose of Investigation	167/279	59.8%	8,000 to 9,000
Use of mobile device for the purpose of Intel Gathering	66/279	23.6%	3,000 to 4,000
Use of mobile device for the purpose of Safeguarding	110/279	39.4%	5,000 to 6,000
Using mobile devices to monitor suspect SM Acc.	33/785	4.2%	1,000 to 2,000
Respondents not aware of i3 (Open Source Team)	410/785	52%	19,000 to 22,000

Not using i3 (Open Source Team) Too Consuming	226/785	28.8%	10,000 to 13,000
Not using i3 (Open Source Team) Own device	166/785	14.8%	5,000 to 7,000

4.4. Policing Dilemmas and Social Media

The previous chapters explored the existence of the alternative hypothesis which stated that police personnel are using personal devices and either personal social media accounts or false personas to access online data that they are using for either investigations, safeguarding, intelligence gathering or a combination of all three (3). In evidencing that these practices are taking place this research also looked at the evidence of why they are occurring and investigated the justifications presented by focus group participants and survey respondents.

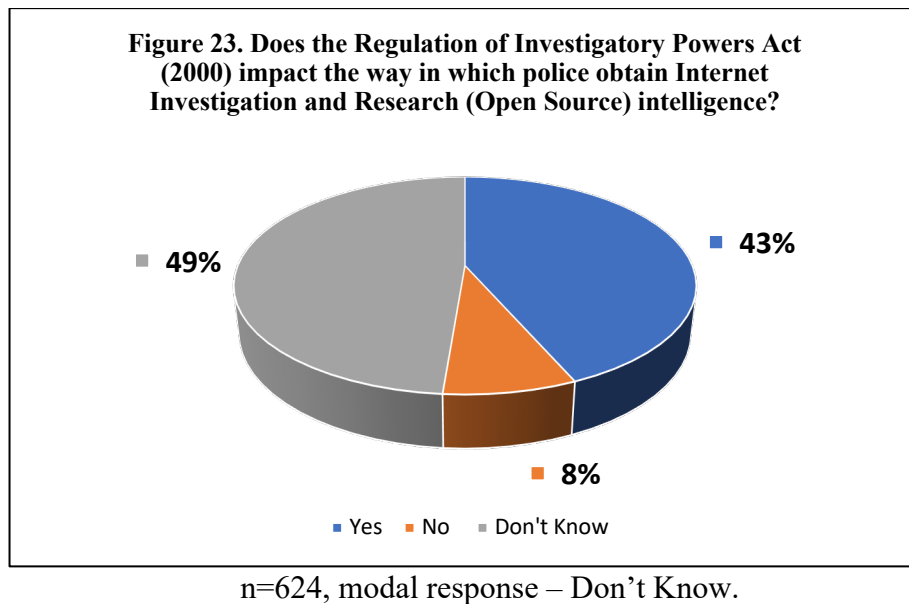
This chapter will consider the policing dilemmas open source and social media create by evaluating MPS personnel’s understanding of their legal, ethical and organisational responsibilities to investigate crime while protecting the public’s rights to privacy. The chapter will then end with a summary of the research findings across the four (4) knowledge questions from the survey.

4.4.1. Legislation: Regulation of Investigatory Powers Act

The last four knowledge questions in the survey were designed to evaluate focus group participants and survey respondent’s knowledge around legislation, MPS policy and the Code of Ethics. While the final question sought to understand how MPS personnel view public data and whether they valued the role security represented by the police and State over the public’s privacy. Across the focus groups it was clear that participants had a limited knowledge of the key legislation contained within the *Regulation of Investigatory Powers Act, 2000* and how it applied to the use of open source, with one participant saying;

Participant: *‘When I first read the question about RIPA, I thought I should know the answer to this.’ – Focus Group 2*

This was echoed in the statistical data obtained in knowledge-based question 1 (**Table 17.**) which asked respondents, ‘Does RIPA impact the way in which police obtain Online Intelligence?’, while **Figure 23.** shows the percentage of answers with the modal response being, ‘Don’t know’ represented by n=304 responses, while n=49 respondents said, ‘No’ it does not impact the way in which the police obtain online intelligence.



Although the modal response was ‘Don’t know’, 43% of respondents answered ‘Yes’ that *Regulation of Investigatory Powers Act (RIPA) 2000* does apply. The limited respondent commentary centred on ‘repeated viewing’ with some awareness of collateral intrusion;

Respondent: ‘Some material that can be obtained from the internet (especially social networking profiles) can be considered private information and will be directed surveillance if repeatedly/frequently viewed.’ – Survey Knowledge Question 1.

Respondent: ‘If you are regularly checking someone’s Facebook account or other social media account, you’re likely to be obtaining private/personal information and experiencing collateral intrusion with regards to the others commenting on the items being posted and potentially breaching RIPA.’ – Survey Knowledge Question 1.

As the knowledge questions were at the end of the survey responses declined with n=624 respondents answering the following questions. This reduction impacts the margin of error, reducing it to 3.9% but remaining within satisfactory parameters. The confidence interval for the population proportion is:

The range for the true population proportion estimates that between N=18,000 and N=21,000 MPS personnel do not know how RIPA impacts the use of open source and social media as a tool for intelligence gathering and investigation. While the limited comments articulated the need to consider ‘repeated viewing’ and ‘collateral intrusion’ there was a lack of understanding about the notions of public and private space with some believing information available on Facebook was all public. In many examples it was clear that the respondents hadn’t recognised that in order to enter many social media sites the user required an account and by entering they were no longer entering an exclusively public domain, but a private one in which the public maintain a certain right to privacy from the state even in a such a public sphere as Facebook as considered by one respondent;

***Participant:** ‘Just because this material is out in the open, does not render it fair game. The Surveillance Commissioners have provided guidance that certain activities will require authority under RIPA, and this includes repeated viewing of what are deemed to be ‘open source’ sites for the purpose of intelligence gathering or data collection.’ – Knowledge Question 1*

As articulated by Brandon (2016) it is one thing for your personal data to be used for marketing purposes, but when the data is being used as intelligence by a representation of the State it is something entirely different. However, the key terminology that needs to be addressed in the legislation is the ambiguity around ‘repeated viewing’ as identified in this research there are a variety of beliefs and understandings in existence as to what constitutes repeated and over what time period. While the guidelines state that the repeated viewing of an individual’s website or social media, which singularly may be considered

as open source material but for the fact that it is being looked at for the purposes of intelligence gathering and data collection, consideration should be given to obtaining the protection of RIPA directed surveillance authority (MPS, 2014c). It is with certainty that those engaging in practices of social media surveillance through the use of personal devices, personal social media accounts and unauthorised false personas will be in breach of RIPA, especially as they are acting covertly. While policy has developed around the concept of repeated viewing, this was never in the original legislation and from a true surveillance point of view is irrelevant; for Fuchs (2011, p.124) surveillance is a control mechanism to oversee and is carried out by watchers or officials signifying a hierarchical power dynamic between those watching and those being watched, but he never mentions the need to watch on more than one occasion. This is a policy measure by the Association of Police Chiefs (ACPO) and designed to mesh the legislation with the needs of the activities being conducted as highlighted by in the Chief Surveillance Commissioner's report 2014-2015,

'Certain activities will require authorisation under RIPA...and this includes repetitive viewing of what are deemed to be 'open source' sites for the purpose of intelligence gathering and data collection.'

4.4.2 MPS Policy

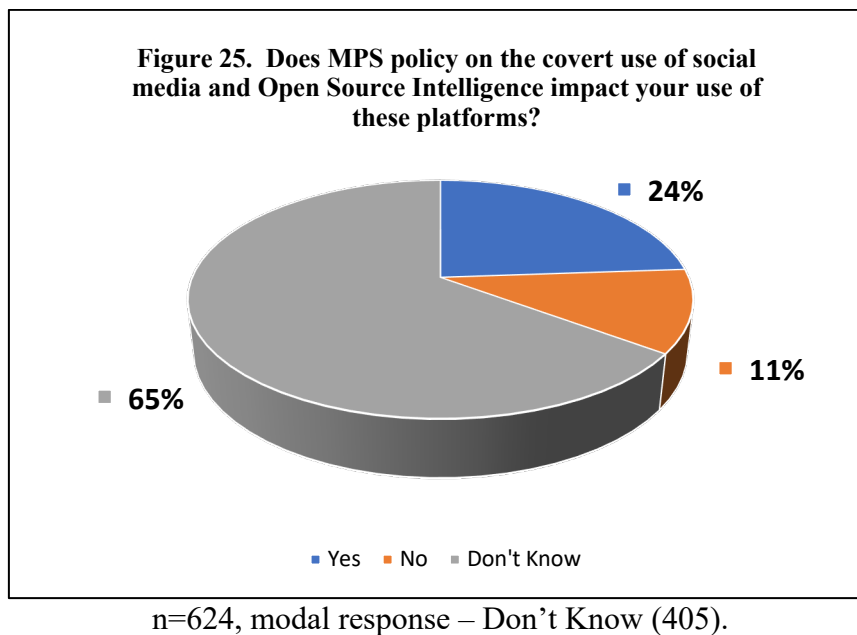
Knowledge question 2. asked, *'How does MPS policy on the covert use of social media and online investigation impact you and the use of these platforms?'* In the focus groups participants were again unsure of what the policies said they could and could not do and although most had received training on the use of social media from the DMC, they felt there was little support to fill the knowledge gap around using social media platforms for more than just engagement saying;

Facilitator: ‘So we have said that these practices (intelligence gathering, etc.) are taking place but are individuals intentionally going against policy?’

Participants: ‘I don’t think they know (police personnel) they are doing anything against the procedures, they think they are allowed to do it.’

– Focus Group 1

Figure 25. represents the percentage of respondent answers to knowledge question 2. in **Table 18.** with the modal answer being ‘Don’t know’ (n=405).



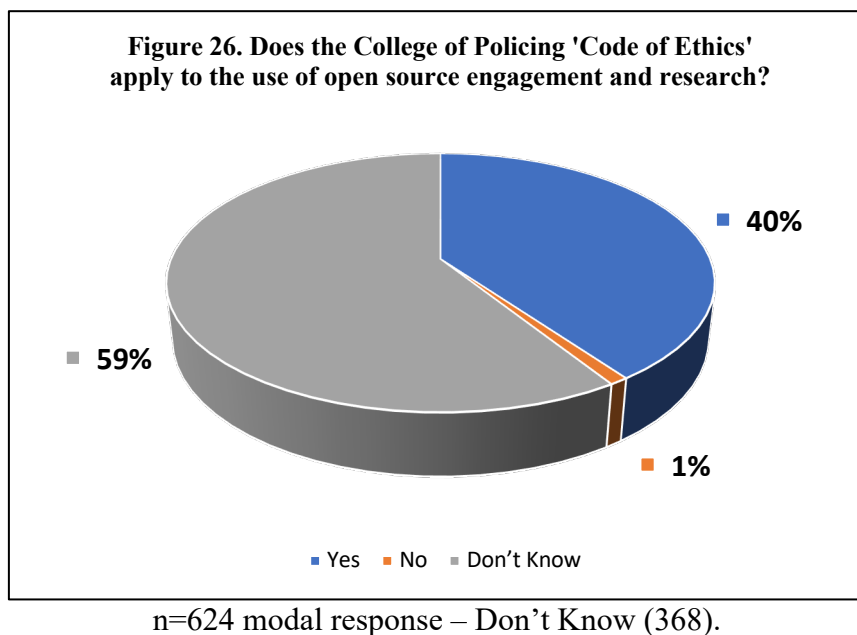
While n=70 respondents answered, ‘No’ MPS policy on the covert use of open source and social media does not impact their use of those platforms. Those respondents who left comments predominantly stated that the policy did not affect their current role and although n=149 said ‘Yes’ the policy did affect their use of these platforms there was little similarity in any of the commentary provided. The confidence interval for the population proportion is based on the modal response of ‘Don’t know’:

The range for the true population proportion estimates that between N=24,000 and N=27,000 MPS personnel do not know how the MPS policy on covert use of social media and online investigation and intelligence impacts their use of these platforms. The lack of

awareness around MPS policy in relation to the use of open source and social media should be of concern to the MPS with the increased use of social media through the practices identified in this research. This lack of understanding supports Bartlett's (2013, p.9) findings that practitioners have no clear legal direction on what is acceptable in terms of conducting social media surveillance investigations and that the interpretation of inadequate legislation has been left to law enforcement to interpret.

4.4.3 College of Policing - Code of Ethics

In knowledge question 3. respondents were asked, 'Does the College of Policing 'Code of Ethics' apply to the use of open source engagement and research?' **Table 19.** shows the frequency of answers with the modal answer being, 'Don't Know' (n=368), while n=6 said 'No' and n=250 said, Yes. **Figure 26.** shows the percentages for the survey responses.



Focus groups were asked if they knew what the Code of Ethics said about the use of open source with the following response;

Participant: 'I wouldn't read that (question 3.) and think I have read the College Policing Code of Ethics.' - Focus Group 2.

Similarly, to knowledge question 2. there were not a significant number of qualitative answers to analyse in the categories of ‘Don’t know’ and ‘No’ and in the category of ‘Yes’ most respondents made sweeping statements about ethics applying to everything. While this may be true few articulated the rudimentary stance stating held by the College of Policing which states, ‘standards that apply to the management of information off line are equally applicable to social media’ (College of Policing, 2014b, p.2). The confidence interval for the population proportion of knowledge question 3. is based on the modal response of ‘Don’t Know’:

The range for the true population proportion estimates that between N=24,000 and N=25,000 MPS personnel do not know what the College of Policing’s Code of Ethics says about the use of social media. While the London Assembly (2013, p.33) says the Metropolitan Police understands that excessive surveillance might stretch public confidence and raise ethical questions, the data in this research suggests that the MPS still have a long way to go demonstrate they truly do understand the potential consequences and will need to positive action to address the current practices identified in this study.

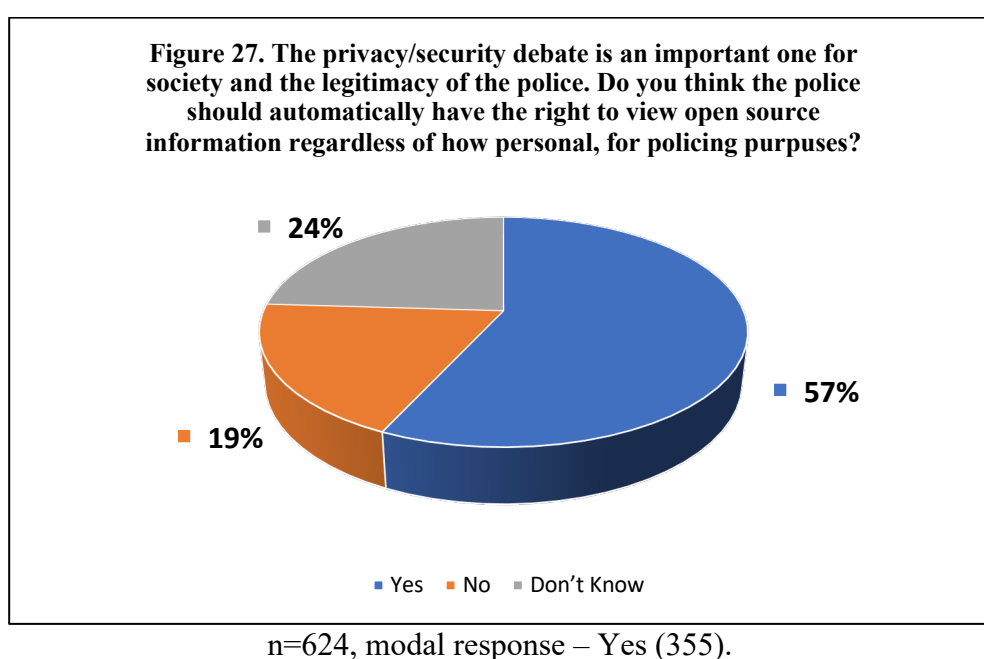
4.4.4 Policing Attitudes towards Privacy/Security

The final question in the survey asks respondents whether they think the police should automatically have the right to view open source information, regardless how personal, for a policing purpose? The question was included to understand how police practitioners viewed the public’s information on the internet. whether personnel constructed a justification for access by articulating a ‘policing purpose?’ The focus group sessions discussed this point;

Participant: ‘If someone’s happy to put their world out on social media ... that’s effectively what they are doing, so is it our job to be responsible for

those people and responsible for Facebook, Twitter and the like. They have privacy settings. We are fighting with both hands behind our backs because we are not confident to use [social media].’ – Focus Group 2.

Table 19. (See appendices) shows the responses to knowledge question 4. with the modal response being ‘Yes’ (n=355 or 57%) who think the police have the right to automatically view open source information regardless of how personal, for a policing purpose while **Figure 27.** presents the percentage of respondents in each category.



The commentary for knowledge question 4 was the most detailed out of all the qualitative data sets and represented an opportunity for personnel to give their opinion. There were three (3) broad themes that the categories fell into as detailed in **Figure 28.** (See appendices). Those respondents who felt that access should be automatic with n=177 comments being made, those who felt that access shouldn't be automatic represented by n=41 comments. The final group who presented their comments with a balanced approach considering the need to respect privacy but recognised the need to access information in the appropriate way who were represented with n=128 comments.

While the commentary was complex and detailed respondents' who stated that access should be automatic made comments such as;

Respondent: *'If people put it out therefore others to see then they should be happy for anyone (the police) to see it.'* - Survey Knowledge Question 4

Respondent: *'Open-source is freely available data; If anyone sticks personal information about themselves on the side of their house it is equally freely available.'* - Survey Knowledge Question 4

Those who felt that it should not be automatically accessible made comments like;

Respondent: *'The police need to be mindful of privacy and freedom of expression in all aspects of policing.'* - Survey Knowledge Question 4

Respondent: *'It would be misused!'* - Survey Knowledge Question 4

While those who articulated the need for balance expressed themselves in the following;

Respondent: *'People are entitled to an expectation of privacy online just as they are on the street. We cannot just go and search someone on the street so we should not be able to search online without reasonable grounds.'* - Survey Knowledge Question 4

Respondent: *'This is incredibly intrusive and shouldn't be used without justification.'* - Survey Knowledge Question 4

The confidence interval for the population proportion of knowledge question 4. Is based upon those who answered 'Yes':

The estimated population proportion range is between N=21,000 and N=24,000 MPS personnel who think the police should have an automatic right to view open source information, regardless how personal, for a policing purpose. The results of this question stand out from the survey as particularly interesting as they presented an opportunity for respondents to openly present complex views on security and privacy while representing some of the most comprehensive qualitative data of the research.

While the primary aim of the research was undertaken to consider police personnel's use of social media and whether almost unfettered access constituted a form of surveillance this element of the research helps to understanding the phenomenon, by exploring the cognitive reasoning for police personnel to engage in such practices.

With 57% of respondent stating police should have access to open source material regardless of how personal for a policing purpose this offers some insight as to why personnel engage in practices such as using their own mobile device and using their own social media accounts. There is a suggestion here that part of the reason for these activities is the cognitive way in which police personnel see the public's data and where they feel responsibility for that data lays, with one respondent saying;

Respondent: *'What do they expect (the public) if they are going to put information on for the world to see.'* - Survey Knowledge Question 4

This suggests in part an internal rationalisation by police practitioners of their actions as acceptable in the context of policing surrounded by a reasonable belief that the public should expect the police to be looking publicly available information. From a practitioner perspective these actions can therefore be argued as legitimate, especially when embroiled in public safety and criminal investigation.

Although privacy is not an absolute right and the police can circumvent normal boundaries with appropriate authority the presence of personal information in the public domain appears to lessen practitioner's consideration for treating it with diligence and respect. Again, as with the counterpart knowledge questions in this section they suggest the need to increase awareness potentially through a combination of training and corporate

communications around both policy and legislation, aiming to improve practitioner’s appreciation for the sensitivities of data privacy, even that which is in the public arena. While there may be a practical argument for accessing such open source information in real time for operational purposes such considerations must strive to look beyond the immediate incident to comprehend the overall impact on policing as an institution of trust.

All of these pieces come together to position themselves in the debate of security vs privacy and while it is the responsibility of government and law enforcement agencies to balance public safety with protecting the privacy rights of the innocent engaging in lawful activities using those same technologies (London Assembly, 2013, p.32; Press Association, 2015). Finally, **Table 27.** summarises the key quantitative findings from this chapter and demonstrates that across each question almost half of respondents didn’t know how legislation, policy or the code of ethics impact the use of open source for investigations (open source) research.

Table 27. Ch. 4.4 Summary of key findings and estimated inferences against MPS Population.

Theme	Survey Response (n)	Percentage (%)	Estimated Population Proportion (N)
Knowledge Q1. RIPA Don’t Know	304/624	49%	18,000 to 21,000
Knowledge Q2. Policy Awareness – Don’t Know	405/634	65%	24,000 to 27,000
Knowledge Q3. CoP– Ethics Don’t Know	368/624	59%	24,000 to 25,000
Knowledge Q4. Security vs Privacy – Automatic	355/624	57%	21,000 to 24,000

Chapter 5. Summary, Recommendations & Concluding Remarks

5.1. Summary

This research began with a null hypothesis that MPS personnel are generating OSINT and specifically SOCMINT within the remit of their training (or lack of training, at level one) without using their personal social media accounts, a false persona or their personal devices. The alternative hypothesis stated, with no training or authority MPS personnel are utilising SOCMINT for policing activities, exploiting access through personal mobile devices, personal social media accounts or by creating false personas to remain covert. These activities constituted a form of social media surveillance that are presented ontologically as for a ‘policing purpose’ by those engaging in the described practices.

Table 28. Summarises the key findings that have been discussed in results and discussion chapter of this research and supports the rejection of the null hypotheses.

Table 28. Summary of all Estimated Population Proportions across research areas

Theme	Survey Response (n)	Percentage (%)	Estimated Population Proportion (N)
No Open Source Training	685/785	87%	30,000 to 39,000
No Social Media Training	606/785	77%	29,000 to 31,000
Level 1. Use of Personal Social Media Account	101/785	13%	4000 to 6000
Level 1. Use of False Persona	24/785	3.5%	800 to 2000
Use of Personal Device	279/785	35.5%	13,000 to 15,000
Use of mobile device for the purpose of Investigation	167/279	59.8%	8,000 to 9,000
Use of mobile device for the purpose of Intel Gathering	66/279	23.6%	3,000 to 4,000
Use of mobile device for the purpose of Safeguarding	110/279	39.4%	5,000 to 6,000
Using mobile devices to monitor suspect SM Acc.	33/785	4.2%	1,000 to 2,000
Respondents not aware of i3 (Open Source Team)	410/785	52%	19,000 to 22,000
Not using i3 (Open Source Team) Too Consuming	226/785	28.8%	10,000 to 13,000
Not using i3 (Open Source Team) Own device	166/785	14.8%	5,000 to 7,000
Knowledge Q1. RIPA Don't Know	304/624	49%	18,000 to 21,000
Knowledge Q2. Policy Awareness – Don't Know	405/634	65%	24,000 to 27,000

Knowledge Q3. CoP– Ethics Don't Know	368/624	59%	24,000 to 25,000
Knowledge Q4. Security vs Privacy – Automatic	355/624	57%	21,000 to 24,000

The specific aims of the research were firstly to identify what open source and social media practices were being employed across the MPS and to establish whether they constituted a form of unauthorised surveillance. Through the use of focus groups and an organisationally distributed survey a combination of qualitative and quantitative evidence was obtained that demonstrated that MPS practitioners are using a combination of personal devices, personal social media accounts and unauthorised false personas in order to carry out online investigations. The research identified that these practices were taking place to varying degrees and that it had been suspected for some time but there had been no verification or quantification due to the lack of internal researcher access. In Egawhary (2019, p. 98) the researcher concludes that their research ‘cannot be said to demonstrate actual police practices’ in the use of social media surveillance which is where this research continues to hold ground and fill an important research gap.

Arguably beyond the original aims of the research but equally important in identifying the presence of these activities was trying to understand the purposes for which they occur and the influences that make them an attractive policing tactic. As a result, this research has established some of the rationale behind the behaviours such as efficiency, restrictive access to official covert ICT and a determination to self-serve. More deeply is the normalising of covert practices that are largely decoupled from mainstream policing (Loftus, 2019, p.2086) as a result of being socially and culturally embedded and accepted in society; they become normalised within a policing context.

The second aim of this research was to identify if there were any gaps in MPS policy that needed to be addressed. Again Egawhary (2019, p. 97) identifies fourteen forces across

the United Kingdom advised staff not to link their personal lives or personal social media accounts to their professional ones. However, this does not go far enough and requires a clear statement that police practitioners should not use their personal accounts for any type of police work/activity. A clear statement which until this research was missing from the MPS policy documents. The clarity on this point in MPS policy ensures police practitioners understand the risks they expose themselves, friends and family members through data leakage, unintended networking and countersurveillance together with the organisational and reputational risks that come with this practice.

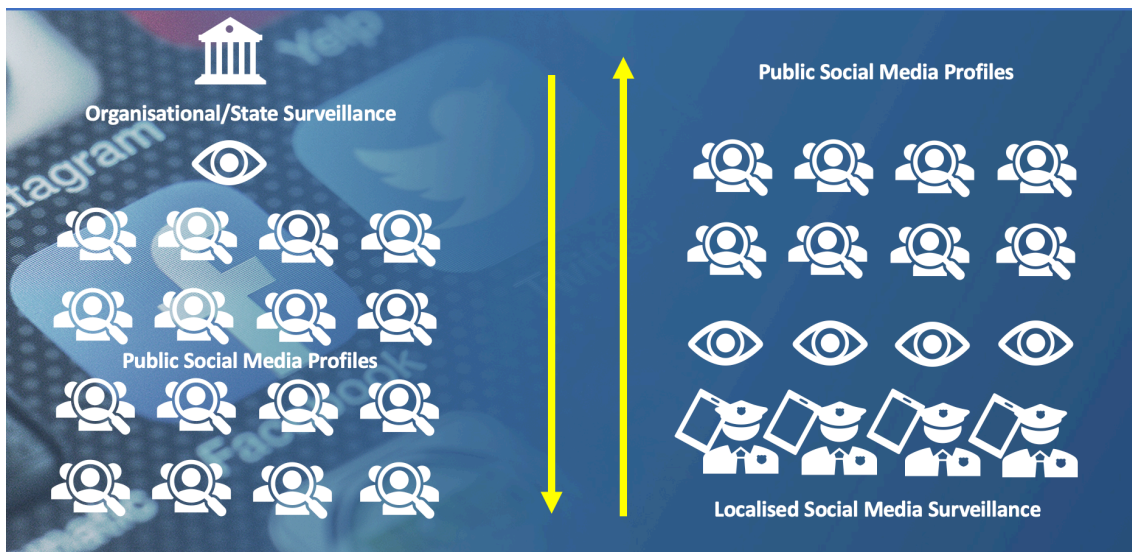
Finally, the third aim of this research was the delivery of a new theoretical interpretation of surveillance in the context of social media and policing. Through the analysis and discussion specific characteristics were identified that made this type of surveillance unique. As a consequence, the term 'localised social media surveillance' was established and considers the 'localised' nature of the surveillance activity to be the central characteristic. While traditional concepts of surveillance focus on panopticon scale and consider the phenomena from a top down perspective there has been a shifting paradigm with the advancement of technology that identifies the rise of lateral or peer to peer surveillance (Ball, Haggerty and Lyon, 2012, p.344). However, this research suggests a bottom up approach to surveillance within policing that operates across both theoretical planes of hierarchical and peer to peer surveillance. For this 'localised' surveillance activity is still being conducted by representatives of the state as power holders within the hierarchy of the social construct but uses social media platforms in a way that mimics lateral surveillance where the balance of power is considered equal by participants through common access to the information published.

The local nature of this surveillance is enhanced by the perceived anonymity practitioners have while conducting it. While the risk-reward aspect of this activity needs further research, commentary suggests that police practitioners conducting these activities see the risks of exposure as marginal compared to the benefits potentially gleaned from the activity itself. In reality it is an unknown risk as the algorithms and data exchanges that work behind the scenes appear to be shrouded in mystery even to Facebook (Tait, 2019) and those algorithms documented have changed regularly since 2004 (Cooper, 2020).

The data suggests PC/DCs predominantly conduct these activities and that they justify their social media use in the context of a policing purpose. The quantitative analysis shows that officers are using their personal devices for a host of legitimate reasons such as 'giving directions' however, some of the reasons clearly fall into the category of surveillance specifically, 'monitoring a suspects social media account'.

The qualitative data goes on to strengthen the idea of this 'local' characteristic by indicating a known connection between the power holder and the audience or subject(s) through local knowledge of their existence. This can be through an investigative introduction, or where the subject is known locally to the power holder and they wish to gain intelligence about them, or where an individual has come to police notice as a result of a safeguarding matter, e.g. as a missing person. The fundamental element here is that the power holder conducting the surveillance is doing so in a targeted fashion isolating particular subject(s) of interest compared to mass surveillance which tends to be sweeping in its collection of data and cover potentially large demographics as illustrated in **Figure 30**.

Figure 30. Comparison between concepts of State Surveillance and Local Social Media Surveillance.



Essential to cases of ‘localised social media surveillance’ are that police personnel are conducting their activities without official organisational support, not line management support but organisational support. Police practitioners are operating outside of the expected standards laid down in legislation and guidance in policy and in many instances those power holders are conducting these activities utilising personal devices but may also be utilising access through other routes such as official ICT infrastructure. Additionally, these activities also see the use of personal social media accounts or false personas to conduct the localised social media surveillance activity.

In every way each part of the practice is kept close or local to the participant in order to remain covert from the audience they are surveilling and the organisation they represent. While this is presented in a policing context, it is clear that ‘localised social media surveillance’ could occur in any organisation deemed to be a power holder or representative of one in a democratic society.

There are clear risks in the use of 'localised social media surveillance' practices as the power holder is working in direct opposition to the official processes and practices established within their organisation. Practitioners not only expose themselves to potential internal disciplinary action for the breaches but risk the reputational damage to their institution which in the case of policing and covert surveillance has already suffered in recent times. But further to this, power holders risk exposing themselves, their personal information and in some instances their friends and family by engaging in practices such as using their own social media account. Raising the question is it worth the potential sacrifice of your own privacy and safety? Additionally, while there may be some limited immediate benefits to the practice of 'localised social media surveillance' such as the retrieval of information quicker than official channels in cases of a high-risk missing persons. Which may be arguably acceptable and down to the discretion of the officer involved; in most cases as demonstrated in this research, the information is for investigation purposes, to locate wanted offenders or gather intelligence. All representing slow time enquiries for which official channels exist to support this work demand and alleviate the need to conduct these enquiries through these localised practices.

5.2. Recommendations

In conducting this research, it has generated a number of recommendations, some of which are already being implemented within the MPS. Firstly, there is a clear need for frontline officers to be able to access open source and social media intelligence. It is inefficient for there to be a limited number of access points for police personnel to conduct these enquiries. As detailed in the literature review currently open source research is processed through the Local Intelligence Teams (LITs), regional Hubs and the central i3 Team (Open Source Team) but these avenues do not provide enough frictionless access to influence frontline practitioners away from their own devices. It is therefore the

recommendation of this research that the MPS consider the availability of official open source access to frontline personnel.

By working in partnership with the Horizons Team this recommendation is currently in the process of being implemented. The removal of standalone terminals that are only located in specific buildings around the MPS estate will be replaced with a virtual platform that allows open source research to be conducted directly from the existing IT infrastructure. While not every officer will have access, the resource will be more widely available than it currently is and offer future scope for further expansion. While the product name cannot be discussed for operational reasons it is a fully audited system which will allow transparency and oversight to ensure the maintenance of standards.

The second recommendation from the research is the targeted intervention and training of the key demographics engaging in 'localised social media surveillance.' Specifically, those of PC/DC rank who have had no training in either the use of open source for investigations and intelligence or social media for the purposes of community engagement. By targeting this demographic with training and guidance the practice of localised social media surveillance could be significantly reduced.

The third recommendation is training and development for all police personnel, with the documented increases in the use of open source and social media combined with the research provided by LexisNexis the frequency of use is set to increase with time. As the results identified there has been significant investment in training to upskill UK officer's knowledge of cybercrime, that includes the use of social media, but there has been no training or support on how to obtain intelligence or carry out investigations using open source and social media. Leaving frontline personnel without training and support will only increase the practices identified by the alternative hypothesis, further embedding them into the normative culture of the MPS.

Recommendation four concerns those service currently available, including the Local Intelligence Teams (LIT's) and the i3 Team (Open Source Team). The survey results identified that 52% of respondents were unaware of the i3 Team, and the most common answers given as to why they were not used centred around respondents not knowing their remit, opening times or how to contact them. As a consequence, the fourth recommendation is for improved communication across the MPS regarding the presence of the i3 (Open Source) Team so that frontline personnel are aware of the resources available to support them. Improved awareness of their capability will support the reduction of localised social media surveillance as personnel refer to them in slow time intelligence checks.

A simple recommendation is the addition to MPS policy that MPS personnel should not utilise their personal social media accounts for the purposes of police work, whether that be an investigation, intelligence gathering or safeguarding. Clarifying this position removes any ambiguity around the acceptableness of this practice and ensures the MPS as an organisation is publishing guidelines that safeguard their employees. This recommendation has been accepted and is now MPS policy.

The final recommendation would be for the collation and distribution of legislation and policy documents in relation to open source research and investigation. They need to be organised and easily accessible so that personnel can refer to them directly. In relation to repeated viewing national guidelines need to be revisited, regardless of the number of times a personal site is accessed or viewed for a policing purpose this is surveillance by the state. The legislation needs to understand and reflect the policing need to access these platforms but ensure appropriate proportionality and necessity are factored into their use.

While this research has been able to explore and answer the three aims it set out to, there have been limitations in the data. Identified earlier the number of untrained level one (1) personnel is lower than the estimates provided by the MPS and is likely to be a knock on effect from promoting the survey to social media trained personnel through the use of Twitter, which equally represented a disproportionately high number of trained personnel. While the knowledge questions provided an insight into personnel's understanding (or lack of) around legislation, policy and ethics in relation to the use of open source; the formulation of the questions and their positioning at the end of the survey may have impacted respondents willingness to provide detailed answers which may have impacted the validity and reliability of the data. Although the reliability coefficient for those knowledge questions was $r=0.92$ it would be prudent for a future study to explore these levels of knowledge independently to ensure an accurate reflection of understanding is captured.

5.3. Concluding Remarks

Future research should be considered across other UK police services as this is an issue that not only impacts the MPS but police services nationally and internationally. Once the MPS has adopted some of the recommendations it would be valuable for a follow up study to evaluate its impact and this would serve as an opportunity to re-evaluate the key findings of this research. However, the key challenge for researchers is access to the data.

The plausible reality will be that regardless of the system implemented there will always be a proportion of personnel who will resort to their personal devices, they are immediately accessible, familiar and offer a covert method of conducting research that is hidden from the organisation they represent. As Loftus (2019, p.2086) concludes covert investigation is a key part of late modern policing...but argues that changes in the visibility of the police have both solidified and accelerated the spread of the covert mindset and practices.'

To this end the role of social media in investigations will continue to grow as the criminals continue to use the social media channels to further their criminal enterprise and share their criminal escapades. Advances in technology will undoubtedly make it easier on law enforcement to leverage this data into their investigative workflow more efficiently and effectively. Training on these tools and technologies will also be critical to ensuring this data is used to its fullest potential and in a secure manner to protect the officer and the agency (LexisNexis, 2014, p.15). However, if we do not tackle the challenges of localised social media surveillance, we risk policing legitimacy through a lack of transparency and respect for the public's privacy for which the police have a responsibility to protect.

References:

- Alderson, P. and Morrow, V. (2011) *The ethics of research with children and young people: A practical handbook*. 2nd edn. London: SAGE Publications Ltd.
- Allen, M. (2017) *The Sage encyclopedia of communication research methods*. Thousand Oaks, CA: SAGE Publications Inc.
- Ashby, M. (2013) 'UK Police on Twitter' *Less Crime*, 19 August. Available at: <http://lesscrime.info/uk-police-on-twitter/> (Accessed: 21 March 2017).
- Association of Chief Police Constables (2013) *Online Research and Investigation*. Available at: <http://library.college.police.uk/docs/appref/online-research-and-investigation-guidance.pdf> (Accessed: 2 March 2018).
- Association of Chief Police Constables (2013) *Guidelines on the safe use of the internet and social media by police officers and police staff*. Available At: <https://www.btp.police.uk/pdf/FOI%20Response%20319-14%20ACPO%20Guidance.PDF> (Accessed: 6 June 2017).
- Ball, K.(ed.), Haggerty, K. and Lyons, D. (2012) *Routledge Handbook of Surveillance Studies*. Oxon: Routledge.
- Baille, S. and Miller, R. (2003) *The A-Z of Social Research*. London: SAGE Publications Ltd.
- Barnour, R. (2007) *Qualitative research kit: Doing focus groups*. London: SAGE Publications Ltd.
- Bartlett, J., Miller, C., Crump, J., and Middleton, L. (2013) Policing in an information age [Online]. Available at: <https://www.demos.co.uk/project/policing-in-an-information-age/> (Accessed: 9 February 2017).
- BBC (2012) *Social media benefits to police investigated*. Available at: <http://www.bbc.co.uk/news/technology-20641190> (Accessed: 13 March 2017).
- BBC (2015) *UK surveillance powers explained*. Available at: <http://www.bbc.co.uk/news/uk-34713435> (Accessed: 13 March 2017).
- Bekkers, V., Edwards, A. and Kool, D. (2013) 'Social media monitoring: Responsive governance in the shadow of surveillance?', *Government Information Quarterly*, 30, pp. 335-342.
- Bickman, L. and Rog, D. (2009) *The SAGE Handbook of Applied Social Research Methods*. Thousand Oaks, CA: SAGE Publications, Inc.
- Bottoms, A. and Tankebe, J. (2012) Beyond procedural justice: A dialogic approach to legitimacy in criminal justice', *The Journal of Criminal Law and Criminology*, 102(1), pp.119-169.
- Brandom, R. (2016) 'Can Facebook and Twitter stop social media surveillance?', *The Verge*, 12 October. Available at:

<http://www.theverge.com/2016/10/12/13257080/police-surveillance-facebook-twitter-instagram-geofeedia> (Accessed: 23 September 2016).

Bowcott, O. and Ball, J. (2014) 'Social media mass surveillance is permitted by law, says top UK official', *The Guardian*, 17 June. Available at: <https://www.theguardian.com/world/2014/jun/17/mass-surveillance-social-media-permitted-uk-law-charles-farr> (Accessed: 23 September 2016).

Brown, I. (2015) 'Social Media Surveillance', *The International Encyclopedia of Digital Communications and Society*: Oxford, pp. 1-7.

Brunger, M., Tong, S. and Martin, D. (2016) *Policing Research – Taking Lessons from Practice*. Oxon: Routledge.

Burgess, M (2018a) 'What is the internet of things? Wired explains', *Wired*, 18 February. Available at: <http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot> (Accessed: 15 March 2018).

Bush, T. (2012) 'Authenticity in research: reliability, validity and triangulation', in Briggs, R.J., Coleman, M., and Morrison, M. (ed.) *Research methods in educational leadership and management*. 3rd Edn. London. Sage Publications Ltd. pp. 75-87.

Cockcroft, T. (2012) *Police Culture - Themes and Concepts*. London: Routledge.

Cameron, D. (2016) 'Twitter cuts ties with second firm police use to spy on social media', *The Daily Dot*, 20 October. Available at: <https://www.dailydot.com/layer8/twitter-snaptrands-geofeedia-social-media-monitoring-facebook> (Accessed: 23 November 2016).

Campbell, K. (2013) 'A call to action: Why we need more practitioner research', *Democracy and Education*, 21(2), pp. 1-8.

Clapham, A. (2015) *Human Rights a Very Short Introduction*. 2nd Edn. Oxford: Oxford University Press.

Cobbe, J. (2018) 'Casting the dragnet: communications data retention under the Investigatory Powers Act', *Public Law: The Constitutional & Administrative Law of the Commonwealth*, January, pp. 10-22. Available at: https://www.researchgate.net/publication/322910623_Casting_the_Dragnet_Communications_Data_Retention_under_the_Investigatory_Powers_Act (Accessed: 20 March 2018).

College of Policing (2013) *The effects of CCTV on crime: What works briefing*. Available at: <http://library.college.police.uk/docs/what-works/What-works-briefing-effects-of-CCTV-2013.pdf> (Accessed: 9 August 2017).

College of Policing (2014a) *Use of social media to monitor large scale events*. Available at: <http://www.college.police.uk/News/archive/2014nov/Pages/Use-of-social-media.aspx> (Accessed: 6 January 2017).

College of Policing (2014b) *Code of ethics*. Available at: http://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf (Accessed: 6 January 2017).

College of Policing (2015) *National policing vision 2016*. Available at: <http://www.college.police.uk/About/Pages/National-policing-vision-2016.aspx> (Accessed: 6 January 2017).

College of Policing (2016) *Undercover policing guidance published*. Available at: <http://www.college.police.uk/News/College-news/Pages/undercover-policing-guide.aspx> (Accessed: 6 January 2017).

College of Policing (2017) *Investigation Communications Strategy*. Available at: <https://www.app.college.police.uk/app-content/investigations/investigative-strategies/communications-strategy/?s=communications+strategy#sources-of-advice> (Accessed: 6 January 2017).

Cooper, P. (2020) *How facebook algorithm works in 2020 and how to make it work for you*. Available At: <https://blog.hootsuite.com/facebook-algorithm/> (Accessed: 18 February 2020).

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

Curtis, B. and Curtis, C. (2011) *Social Research: A practical introduction*. London: SAGE Publications Ltd.

Davies, M. (2016) 'To What Extent Can We Trust Police Research?: Examining trends in research 'on', 'with', 'by' and 'for' the police', *Nordisk Politiforkning*. 3(6) pp. 154-164.

Davies, P., Francis, P., and Jupp, V. (2011) *Doing Criminological Research*. 2nd Edn. London: Sage.

Denscombe, M. (2014) *The good research guide: For small-scale social research projects*. 5th Edn. Maidenhead: Open University Press.

Denzin, N. K. (1989) *The Research Act: A theoretical introduction to sociological methods*. (3rd edn). Englewood Cliffs, NJ: Prentice Hall.

Dingwall, R., and McDonnell, B. (2015) *The SAGE handbook of research management*. London: SAGE Publications Ltd.

Egawhary, E. M. (2019) The Surveillance Dimensions of the Use of Social Media by UK Police Forces. *Surveillance & Society* 17(1/2). pp.89-104. Available at: <https://pdfs.semanticscholar.org/5a43/c9183739724afe6552a528ecfe5d59353ca8.pdf> (Accessed: 20 March 2020)

Evans, C. (2018a) *Human rights news, views and info*. Available at: <https://rightsinfo.org/government-defeated-snoopers-charter-ruled-unlawful/> (Accessed: 4 May 2018).

- Evans, R. (2018b) 'Undercover policing inquiry will not deliver final report before 2023', *The Guardian*, [Online]. Available at: <https://www.theguardian.com/uk-news/2018/may/10/undercover-policing-inquiry-will-not-deliver-final-report-before-2023> (Accessed: 5 November 2018).
- Faubion, J. (2002) *Michel Foucault power – Essential works of Foucault 1954-1984*. London: Penguin Group.
- Fern, E. F. (2001) *Advanced Focus Group Research*, Thousand Oaks, CA: SAGE Publications Inc.
- Fielding, N. and Caddick, N. (2017) *Police Communications and Social Media* [Online]. Available at: <http://upsi.org.uk/oscar> (Accessed: 10 May 2017).
- Fike, D. (2015) 'Why Facebook does not reflect reality', *Possibility of Change*, 18 September. Available at: <https://possibilitychange.com/facebook-does-not-reflect-reality/#respond> (Accessed: 4 May 2018).
- Fisher, T. (2012) 'The UK and Social Media. Partners in Crime?', *Social Media Today*, 4 October. Available at: <http://www.socialmediatoday.com/content/uk-police-and-social-media-partners-crime> (Accessed: 2 February 2017).
- Flick, U. (2018) 'Triangulation in data collection' in Flick, U. (ed) *The Sage Handbook of qualitative data collection*. London: Sage Publishing Ltd. pp. 527-544.
- Fox, M., Martin, P., and Green, G. (2007) *Doing Practitioner Research*. London: Sage.
- Frey, B. (2018) *The SAGE encyclopedia of educational research, measurement and evaluation*. Thousand Oaks, CA: SAGE Publications Inc.
- Fricker, R. and Schonlau, M. (2013) 'Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature', *Sage Journals*. 2, pp.1-20. Available At: <https://methods.sagepub.com/base/download/BookChapter/sage-internet-research-methods/n21.xml> (Accessed: 9 January 2019).
- Fuchs, C., Boersma, K., Albrechtslund, A., and Sandoval, M. (2012) *Internet and Surveillance – The Challenges of Web 2.0 and Social Media*. Oxon: Routledge.
- Fuchs, C. and Trottier, D. (2013) *Social media surveillance and society* [Online]. Available at: http://www.projectpact.eu/privacy-security-research-paper-series/privacy-security-research-paper-series/%238_Privacy_and_Security_Research_Paper_Series.pdf (Accessed: 12 December 2016).
- Fuchs, C. (2017) *Social media: A critical reflection*. 2nd edn. London: SAGE Publications Ltd.
- Given, L. M. (2008) *The SAGE encyclopedia of qualitative research methods*. Thousand Oaks, CA: SAGE Publications
- Gottfredson, M. and Hirschi, T (1990) *A general theory of crime*. Stanford, California: Stanford University Press.

Great Britain. HMIC (2012) *Policing in austerity: One year on*. [Online]. Available at: <https://www.justiceinspectors.gov.uk/hmic/media/policing-in-austerity-one-year-on.pdf> (Accessed: 27 January 2017).

Great Britain. HMIC (2014) *State of Policing the assessment of policing in England and Wales 2013/2014*. [Online]. Available at: <https://www.justiceinspectors.gov.uk/hmicfrs/wp-content/uploads/state-of-policing-13-14.pdf> (Accessed: 14 January 2018).

Great Britain. HMIC (2015a) *Real lives, real crimes: A study of digital crime and policing*. [Online]. Available at: <https://www.justiceinspectors.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf> (Accessed: 14 March 2017).

Great Britain. HMIC (2015b) *In harm's way: The role of the police in keeping children safe* [Online]. Available at: <https://www.justiceinspectors.gov.uk/hmicfrs/wp-content/uploads/in-harms-way.pdf> (Accessed: 20 March 2017).

Great Britain. HMIC (2017) *Use of the Police National Computer: An Inspection of the ACRO Criminal Records Office*. [Online]. Available at: <https://www.justiceinspectors.gov.uk/hmicfrs/wp-content/uploads/police-national-computer-use-acro-criminal-records-office.pdf> (Accessed: 23 January 2018).

Great Britain. House of Commons (2018) *Police Service Strength*. London: House of Commons Library (00634). [Online]. Available At: <http://researchbriefings.files.parliament.uk/documents/SN00634/SN00634.pdf> (Accessed: 24 September 2018).

Great Britain. Home Office (2018) *Covert Surveillance and Property Interference – Revised Codes of Practice* [Online]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf (Accessed: 7 November 2018).

Great Britain. Home Office (2019) *Police Workforce England and Wales, 30th September 2018*. [Online]. Available At: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/772792/police-workforce-sep18-hosb0219.pdf (Accessed 10 February 2019).

Great Britain. London Assembly (2013) *Smart Policing: How the Metropolitan Police Service can make better use of technology*. [Online]. Available at: https://www.london.gov.uk/sites/default/files/gla_migrate_files_destination/Police%20technology%20report%20-%20Final%20version.pdf (Accessed: 18 October 2016).

Halpern, D. (2015) *Inside the Nudge Unit*. UK: Penguin Random House.

Greener, I. (2011) *Designing social research: A guide for the bewildered*. London: SAGE Publications Ltd.

Greenfield, P. (2018) 'The Cambridge Analytica files: The story so far', *The Guardian*, 26 March. Available at: <https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far> (Accessed: 26 March 2018).

Gubrium, J. and Holstein, J. (2001) Handbook of interview research. Thousand Oaks, CA: SAGE Publications Inc.

Guest, G., Namey, E. and Mitchell, M. (2013) *Collecting qualitative data: A field manual for applied research*. London: SAGE Publications, Ltd.

Hanson, W. (2011) 'How social media is changing law enforcement', *Government Technology*, 2 December. Available at: <http://www.govtech.com/public-safety/How-Social-Media-Is-Changing-Law-Enforcement.html> (Accessed: 3 June 2017).

Hewson, C., Vogel, C., and Laurent, D. (2016) *Internet research methods*. London: SAGE Publications Ltd.

Human Rights Act 1998, Ch 42. Available At: <http://www.legislation.gov.uk/ukpga/1998/42/contents> (Accessed: 15 June 2017).

Hill, R. (2017) *The Register*. Available at: https://www.theregister.co.uk/2017/12/21/uk_council_staff_stalking_citizens_social_media_surveillance_laws/ (Accessed: 10 March 2018).

Homolova, P. (2018) 'Theories of Police Legitimacy – Its Source and Effects', *Studia Sociologica* 2, pp.93-113. Available at: http://www.cupress.cuni.cz/ink2_stat/dload.jsp?prezMat=111558 (Accessed: 12 November 2018).

Interception of Communications Commissioner (2017) *Report of the Interception of Communications Commissioner: Annual Report*. [Online]. Available at: https://www.ipco.org.uk/docs/CCS207_CCS1217634744-1_IOCCO_ARA_16-17.pdf (Accessed: 10 March 2018).

Investigatory Powers Act 2016, Ch 25. Available At: <http://www.legislation.gov.uk/ukpga/2016/25/introduction/enacted> (Accessed: 20 April 2018).

IPCO. (2018) *Investigatory Powers Commissioners Office*. [Online]. Available at: www.ipco.org.uk. (Accessed: 10 November 2018).

Jackson, E. (2013) 'Choosing a methodology: Philosophical underpinning', *Practitioner in Higher Education*, 7(1), pp. 49-62.

Keusch, F. (2012) 'How to increase response rates in list-based web survey samples', *Science Computer Review*, 30(3), pp.380-388.

Jupp, V. (2006) *The SAGE dictionary of social research methods*. London: SAGE Publications Ltd.

Kaplan, A. and Haelein, M. (2010) 'Users of the world, unite! The challenges and opportunities of social media', *Business Horizons*, 53, pp. 59-68.

Kaufman (2016) 'Social Media Surveillance Could Have a Devastating Impact on Free Speech. Here's Why', *Mic.com*, 19 January. Available at:

<https://mic.com/articles/132756/social-media-surveillance-could-have-a-devastating-impact-on-free-speech-here-s-why#.wX4cwt5JX> (Accessed: 10 September 2017).

Kara, H. (2012) *Research and evaluation for busy practitioners: A time saving guide*. Available at:

https://www.amazon.co.uk/gp/product/B009VBCPIE/ref=oh_aui_d_detailpage_o00_?ie=UTF8&psc=1 (Downloaded: 6 September 2018).

Kavanaugh, A., Fox, E., Sheetz, S., Yang, S., Tzy Li, L., Shoemaker, D., Natsev, A., and Xie, L. (2012) 'Social media use by Government: From the routine to the critical', *Government Information Quarterly*, 29, pp. 480-491.

Holyk, G.G. (2008) 'Questionnaire Design', in Lavrakas, P.J. (ed) *Encyclopedia of survey research methods*. Thousand Oaks, CA: SAGE Publications Inc, pp. 657-659.

Hugick, L. and Best, J. (2008) 'Questionnaire Length', in Lavrakas, P.J. (ed) *Encyclopedia of survey research methods*. Thousand Oaks, CA: SAGE Publications Inc, p.660.

Kose, H., Han, T., and Bakan, U (2010) 'The Challenging Nature of Communication and Surveillance Phenomena at Synopticon Stage', *Journal of Alternative Perspectives in the Social Sciences*, 2(2), pp. 253-549.

Kvale, S. (2007) *Introduction to interview research*. London: SAGE Publications Ltd.

Lavrakas, P. (2011) 'Internal Validity' in Lavakas, P. (ed). *Encyclopedia of survey research methods*. Thousand Oaks, CA: SAGE Publications Inc, pp. 346-351.

Laws, S., Harper, C., and Marcus, R. (2003) *Research for development*. London: SAGE Publications Ltd.

LexisNexis (2012) *Law enforcement personnel use of social media in investigations: Summary of findings* [Online]. Available at: <https://risk.lexisnexis.com/insights-resources/white-paper/2012-law-enforcement-social-media> (Accessed 10 January 2019).

LexisNexis (2014) *Social media use in law enforcement* [Online]. Available at: <https://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf> (Accessed: 12 January 2017).

Liamputpong, P. (2011) *Focus group methodology: Principles and practice*. London: SAGE Publications, Ltd.

Liberty (2010) *Summary of surveillance powers under RIPA*. Available at: <https://www.libertyhumanrights.org.uk/sites/default/files/introduction-to-ripa-august-2010.pdf> (Accessed: 15 June 2017).

Liberty (2014) Briefing on 'Internet Connection Records' in the Investigatory Powers Bill for Report Stage in the House of Lords. Available at: <https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%20briefing%20on%20ICRs%20for%20Report%20Stage%20in%20the%20House%20of%20Lords.pdf> (Accessed: 18 November 2018).

- Litwin, M. (1995) *How to measure survey reliability and validity*. Thousand Oaks, CA: SAGE Publications Inc.
- Loftus, B. (2019) 'Normalizing covert surveillance: the subterranean world of policing', *The British Journal of Sociology*, 70(5), pp. 2070-2091.
- Lyon, D. (1991) 'Bentham's Panopticon: From Moral Architecture to Electronic Surveillance', *Queen's Quarterly*, 98(3), pp. 596-617.
- Lyon, D. (1998) 'The world-wide web of surveillance: The internet and off world power flows', *Information, Communication and Society*, 1(1), pp. 91-105.
- Lyon, D. (2003a) *Surveillance as Social Sorting – Privacy, Risk and Digital Discrimination*. Oxon: Routledge.
- Lyon, D. (2003b) *Surveillance after 9/11*. Oxford: Blackwell Publishing.
- Longstreet, P. and Brooks, S. (2017) 'Life Satisfaction: A key to managing internet and social media addiction', *Technology in Society*, 50, pp. 73-77.
- Mariampolski, H. (2001) *Qualitative market research*. Thousand Oaks, CA: SAGE Publications Inc.
- Marwick, A. (2012) 'The public domain: Social surveillance in everyday life', *Surveillance and Society*, 9(4), pp. 378-393.
- Mathiesen, T. (1997) 'The viewer society – Michael Foucault's 'Panopticon' revisited', *Theoretical Criminology*, 1(2), pp. 215-234.
- Mayer-Schonberger V. and Cukier, K. (2017) *Big Data*. London: John Murray Publishers.
- McMullen, T. (2015) 'What does the panopticon mean in the age of digital surveillance', *The Guardian*, [Online]. Available at: <https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham> (Accessed: 12 November 2018).
- Metropolitan Police Service. (2003) *Annual Report 202/03*. Available at: <http://policeauthority.org/metropolitan/downloads/publications/annualrep2002-03.pdf> (Accessed: 20 February 2019).
- Metropolitan Police Service. (2013) *Using social media for professional reasons*. Available at: https://www.met.police.uk/globalassets/foi-media/disclosure_2016/july_2016/information-rights-unit---information-concerning-the-use-of-social-media-within-the-mps-from-january-2012---june-2016 (Accessed: 10 January 2018).
- Metropolitan Police Service. (2014a) MPS Media Policy. Available at: <https://www.met.police.uk/globalassets/foi-media/policies/met-hq---portfolio--planning---mps-media-policy> (Accessed: 10 June 2017).

Metropolitan Police Service (2014b) *Internet and social media use in the MPS: Guidance*. Available at: https://www.met.police.uk/globalassets/foi-media/disclosure_2017/september_2017/information-rights-unit---updatedadditional-guidance-and-policy-on-the-use-of-open-source-intelligence-and-or-social-media-monitoringintelligence (Accessed: 10 December 2016).

Metropolitan Police Service. (2014c) *Covert Governance and Intelligence Compliance*. Available at: https://www.met.police.uk/globalassets/foi-media/disclosure_2016/march_2016/information-rights-unit---mps-policy-for-officers-and-staff-when-monitoring-social-networking-accounts-as-part-of-an-enquiry (Accessed: 12 January 2017).

Metropolitan Police Service. (2015a) *Media Policy Toolkit*. Available at: https://www.met.police.uk/globalassets/foi-media/disclosure_2015/august_2015/information-rights-unit---policy-documents-and-guidelines-between-mps-press-officers-and-journalists-on-requesting-information (Accessed: 10 June 2017).

Metropolitan Police Service. (2015b) *Surveillance Policy*. Available at: <https://www.met.police.uk/globalassets/foi-media/policies/met-hq---portfolio--planning---surveillance-policy> (Accessed: 10 June 2017).

Metropolitan Police Service. (2016) *Total notifiable offences where there features in the classification method field names of popular social media sites*. Available at: https://www.met.police.uk/globalassets/foi-media/disclosure_2016/may_2016/information-rights-unit---recorded-crimes-involving-social-media-from-2011-2015 (Accessed: 10 June 2017).

Metropolitan Police Service. (2017) *Top ten examples of police social media*. Available at: <http://apcomm.org.uk/wp-content/uploads/2017/08/Top-10-examples-of-police-social-media-and-why-they-work.pdf> (Accessed: 9 September 2017).

Metropolitan Police Service. (2017) *Digital Policing Strategy*. Available At: <https://www.met.police.uk/SysSiteAssets/media/downloads/met/about-us/one-met-digital-policing-strategy-2017-2020.pdf> (Accessed: 2 March 2018).

Mitting, J. (2015) *Undercover Policing Inquiry* [Online]. Available at: <https://www.ucpi.org.uk/wp-content/uploads/2015/07/Opening-Remarks.pdf> (Accessed: 5 November 2018).

MOPAC (2019) *Workforce Dashboard*. Available At: <https://www.london.gov.uk/what-we-do/mayors-office-policing-and-crime-mopac/data-and-statistics/policing/workforce-dashboard> (Accessed: 10 March 2019).

Morgan, D. and Hoffman, K. (2018) *The SAGE handbook of qualitative data collection*. London: SAGE Publications Ltd.

Morgan, D. (2019) *Basic and advanced focus groups*. Thousand Oaks, CA: SAGE Publications Inc.

- Morris, A. (2015) *A practical introduction to in-depth interviewing*. London: SAGE Publications Ltd.
- Nishishiba, M., Jones, M., and Kraner, M. (2014) *Research methods and statistics for public and non-profit administrators: A practical Guide*. London: SAGE Publications Ltd.
- O'Connor, C. (2017) 'The police on Twitter: image management, community building, and implications for policing in Canada.', *Policing and Society: An International Journal of Research and Policy*, pp. 899-912. Available at: <http://www.tandfonline.com/doi/ref/10.1080/10439463.2015.1120731?scroll=top> (Accessed: 12 December 2017).
- O'keefe, C. and Chakrabarti, M. (2016) 'What police surveillance of social media could mean for you', *Radio Boston*, [Podcast]. 22 December. Available at: <http://www.wbur.org/radioboston/2016/12/22/social-surveillance-police> (Accessed at: 15 February 2017).
- OSCAR. (2017a) The challenges of open source [Online]. Available at: <http://upsi.org.uk/oscar> (Accessed: 10 May 2017).
- OSCAR. (2017b) Data driven information, knowledge driven identification [Online]. Available at: <http://upsi.org.uk/oscar> (Accessed: 10 May 2017).
- OSCAR. (2017c) Police Communications and Social Media [Online]. Available At: <http://upsi.org.uk/oscar/> (Accessed: 10th May 2017).
- O'Rielly, K. (2009) *Key concepts in ethnography*. London: SAGE Publications Ltd.
- O'Rielly, M., Ronzoni, P., and Dogra, N. (2013) *Research with children*. London: SAGE Publications Ltd.
- Paulus, T., Lester, J., and Dempster, P. (2014) *Digital tools for qualitative research*. London: SAGE Publications Ltd.
- Plano Clark, V. and Ivankova, N. (2016) *Mixed methods research: A guide to the field*. Thousand Oaks, CA: SAGE Publications
- Picazo-Vela, S., Gutierrez-Martinez, I. and Luna-Reyes, L. (2012) 'Understanding risks, benefits and strategic activities of social media applications in the public sector', *Government Information Quarterly*, 29, pp. 504-511.
- Procter, R., Crump, J., Karstedt, S., Voss, A., and Cantijoch, M. (2013) 'Reading the riots: What were the police doing on Twitter?', *Policing and Society: An International Journal of Research and Policy*, 23(4), pp. 413-436.
- Press Association. (2012) 'Social media-related crime reports up 780% in four years', *The Guardian*, [Online]. Available at: <https://www.theguardian.com/media/2012/dec/27/social-media-crime-facebook-twitter> (Accessed: 20 March 2018).

Press Association. (2015) 'Police seek powers to access browsing history of UK computer users', *The Guardian*, [Online]. Available at: <https://www.theguardian.com/uk-news/2015/oct/30/police-seek-powers-to-access-browsing-history-of-uk-computer-users> (Accessed: 17 March 2017).

Regulation of Investigatory Powers Act 2000, Ch 23. Available at: <https://www.legislation.gov.uk/ukpga/2000/23/contents> (Accessed: 15 June 2017).

ROSA (2017) *Understanding and using open source resources for law enforcement operational and analytical activities* [Online]. Available at: http://emergencymanagement.senate.ca.gov/sites/emergencymanagement.senate.ca.gov/files/real_time_and_open_source_analysis_resource_guide.pdf (Accessed: 8 January 2018).

Ross, N. (2014) 'Why 30 years of Crimewatch is still a force for good', *The Telegraph*, [Online]. Available at: <https://www.theguardian.com/uk-news/2015/oct/30/police-seek-powers-to-access-browsing-history-of-uk-computer-users> (Accessed: 8 December 2017).

Roufa, T. (2016a) 'The use of social media monitoring tools for law enforcement', *The Balance*, 17 July [Online]. Available at: <https://www.thebalance.com/social-networking-and-law-enforcement-974548> (Accessed: 19 January 2017).

Roulston, K., and Choi, M. (2018) 'Qualitative Interviews' in Flick, U. (ed.) *The Sage handbook of qualitative data collection*. London: Sage Publications Ltd, pp. 233-249.

Ruel, E., Wagner, W., and Gillespie, B.J. (2016) *The practice of survey research*. Thousand Oaks, CA: SAGE Publications Inc.

Sayre, G. and Dahling, J. (2015) 'Surveillance 2.0: How personality qualifies reactions to social media monitoring policies', 90, pp. 254-259.

Schneider, C. (2016) 'Police presentational strategies on Twitter n Canada', *Policing and Society: An International Journal of Research and Policy*, 26(2), pp. 129-147.

Sherman, L. (2013) 'The rise of evidence-based policing: Targeting, testing and tracking', *The University of Chicago Press Journals*, 42(1), pp.377-451. Available at: <https://www.journals.uchicago.edu/doi/abs/10.1086/670819> (Accessed: 10 January 2019).

Sterba, S., and Foster, M. (2008) 'Self-Selected Samples', in Lavrakas, P.J. (ed) *Encyclopedia of survey research methods*. Thousand Oaks, CA: SAGE Publications Inc, pp. 807-808.

Sweeney-Burke, J. (2015) *Social Media Under Investigation – Law Enforcement and the Social Web*. Belfast: Book Hub Publishing.

Solove, D. (2011) *Nothing to Hide*. New Haven and London: Yale University Press.

Tan, E. (2018) 'Are the techniques used by Cambridge Analytica part of the value exchange that social media users must accept?', *Campaign Live*, 21 March. Available at: <https://www.campaignlive.co.uk/article/techniques-used-cambridge-analytica-part>

value-exchange-social-media-users-accept/1459976?bulletin=campaign_media_bulletin
(Accessed 26 March 2018).

Sue, V. and Ritter, L. (2012) *Conducting online surveys*. 2nd Edn. Thousand Oaks, CA: SAGE Publications Ltd.

Tait, A. (2019) *Why does facebook recommend friends I have never met?* Available At: <https://www.wired.co.uk/article/facebook-people-you-may-know-friend-suggestions>
(Accessed 12 December 2019).

Tang, Y. and Joiner, C. (2006) *Synergic inquiry, paradigms and other methodologies*. Thousand Oaks, CA: SAGE Publications.

Tashakkori, A., and Teddlie, C. (2010) *SAGE handbook of mixed methods in social and behavioral research*. Thousand Oaks, CA: SAGE Publications, Inc.

Toepoel, V. (2017) *The SAGE handbook of online research methods*. London: SAGE Publications Ltd.

The Police Foundation (2008) *Too much surveillance*. Available at: <http://www.police-foundation.org.uk/events/oxford-policing-policy-forum/2008-too-much-surveillance>
(Accessed: 8 January 2017).

The Police Foundation (2014) *Police use of social media*. Available at: http://www.police-foundation.org.uk/uploads/catalogerfiles/police-use-of-social-media/Social_media_briefing_FINAL.pdf (Accessed: 8 January 2017).

Thomas, M. (2003) *Blending qualitative and quantitative research methods in thesis and dissertations*. Thousand Oaks, CA: SAGE Publications, Inc.

Toepoel, V. (2016) *Doing Surveys Online*. London: SAGE Publications Ltd.

Travis, A. (2018) 'UK mass digital surveillance regime ruled unlawful', *The Guardian*, 30 January. Available at: <https://www.theguardian.com/uk-news/2018/jan/30/uk-mass-digital-surveillance-regime-ruled-unlawful-appeal-ruling-snoopers-charter> (Accessed: 6 March 2018).

Tripp, D. (2005) 'Action research: A methodological introduction', *Educação e Pesquisa*, 31(3), pp. 443-466.

Trottier, D. (2013) *Social Media as Surveillance – Rethinking visibility in a converging world*. Oxon: Routledge.

Trottier, D. (2014) 'Police and user led investigations on social media', *Journal of Law, Information and Science*, 23(1), pp.75-96.

Trottier, D. (2015a) 'Open source intelligence, social media and law enforcement: Visions, constraints and critiques', *European Journal of Cultural Studies*, 18(4-5), pp. 530-547.

Tuckel, P., Leppo, E., and Kaplan, B. (1992) 'Focus Groups Under Scrutiny: Why people go and how it affects their attitudes towards participation', *Marketing Research*, 4(2), pp.12-18

Vehovar, V. and Manfreda, L. (2017) *The SAGE handbook of online research methods*.

Wacks, R. (2015) *Privacy: A short introduction*. Oxford: University Press. London: SAGE Publications Ltd.

Wahyuni, D. (2012) 'The research design maze: Understanding paradigms, cases, methods and methodologies', *Journal of Applied Management*, 10(1), pp. 69-80.

Walsh, B. and Farrington, D. (2007) *Closed-circuit television, surveillance and crime prevention* [Online]. Available at: http://www.crim.cam.ac.uk/people/academic_research/david_farrington/cctvsw.pdf (Accessed: 15 February 2018).

Walters, G. (2012) *Social media and law enforcement: Potential Risks*. [Online]. Available at: <https://leb.fbi.gov/2012/november/social-media-and-law-enforcement-potential-risks> (Accessed: 12 January 2017).

Weinfass, I. (2017) *Police Oracle* Available at: https://www.policeoracle.com/news/police_finance/2017/Jan/26/officer-numbers-are-still-falling_93976.html (Accessed: 21 March 2017).

Williams, M., Edwards, A., Housley, W., Burnap, P., Rana, O., Avis, N., Morgan, J., and Sloan, L. (2013) 'Policing cyber-neighbourhoods: Tension monitoring and social media networks', *Policing and Society: An international Journal of Research and Policy*, 23(4), pp. 461-481. *Taylor and Francis* [Online]. Available at: <https://www.tandfonline.com/doi/abs/10.1080/10439463.2013.780225> (Accessed: 15 June 2017).

Willis, G. (2016) *The SAGE handbook of survey methodology*. London: SAGE Publications Ltd.

Bibliography

- Andreassen, C., Pallessen, S. and Griffiths, M. (2017) 'The relationship between addictive use of social media, narcissism and self-esteem', *Addictive Behaviours*, 64, pp. 287-293.
- Barfield, T. (2017) 'Peelian principles of policing: How to get the public on your side: An informed public is more likely to support us', *PoliceOne.com*, 10 February. Available at: <https://www.policeone.com/community-policing/articles/289620006-Peelian-principles-of-policing-How-to-get-the-public-on-your-side> (Accessed: 3 June 2017).
- Black Mirror* (2017) Netflix, 21 October.
- Burgess, M. (2018b) 'What is GDPR? The summary guide to GDPR compliance in the UK', *Wired*, 8 May. Accessible at: <http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018> (Accessed: 10 May 2018).
- Burrows, T. (2014) 'Sir Robert Peel's social media principles of modern policing', *Walking the Social Media Beat*, 30 June. Available at: <http://walkingthesocialmediabeat.com/sir-robert-peels-social-media-principles-of-modern-policing-smday> (Accessed: 3 June 2017).
- Chatfield, T. (2012) *50 ideas you really need to know – digital*. London: Quercus
- Children's Commissioner (2018) *Life in likes': Children's Commissioner report into social media use among 8-12 year olds*. Available at: <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/01/Childrens-Commissioner-for-England-Life-in-Likes.pdf> (Accessed: 2 February 2018).
- Clementine, K. (2017) 'Metropolitan Police boroughs will decrease to 12 'Basic Command Units' in response to £325m of government cuts', *Get West London*, 12 February. Available at: <https://www.getwestlondon.co.uk/news/west-london-news/metropolitan-police-boroughs-decrease-12-14279558> (Accessed: 20 March 2018).
- Cole, H. (2018) 'Throw the facebook at em' Over 300 cops and police staff disciplined for social media offences including grooming and sharing extreme porn', *The Sun*, 19 January [Online]. Available at: <https://www.thesun.co.uk/news/5384026/over-300-cops-and-police-staff-disciplined-for-social-media-offences-including-grooming-and-sharing-extreme-porn/> (Accessed: 27 February 2018).
- Bartsch, M. and Dienlin, T. (2015) 'Control your Facebook: An analysis of online privacy literacy', *Computers in Human Behaviour*, 56, pp. 147-154.
- Couts, A. (2013) 'Forget Silk Road, assassination market is the new 'deep web' nightmare', *Digital Trends*, 19 November. Available at: <https://www.digitaltrends.com/web/bitcoin-funded-assassination-market-website/> (Accessed: 20 March 2018).
- Dickey, M. (2016) 'Police are increasingly using social media surveillance tools', *Techcrunch*, 23 September. Available at: <https://techcrunch.com/2016/09/23/police-are-increasingly-using-social-media-surveillance-tools> (Accessed: 23 September 2016).

'Documentary television series about policing' (2016) *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Category:Documentary_television_series_about_policing (Accessed: 20 December 2017).

Dowd, L (2017) 'Online fraud most prevalent crime in England and Wales', *Sky News*, 6 December. Available at: <https://news.sky.com/story/online-fraud-most-prevalent-crime-in-england-and-wales-11158370> (Accessed: 20 January 2018).

Entis, L. (2014) 'The crazy, cool and unsettling ways police are using social media', *Entrepreneur*, 2 May. Available at: <https://www.entrepreneur.com/article/233604> (Accessed: 20 November 2016).

Gallagher, R. and Syal, R. (2011) 'Met police using surveillance system to monitor mobile phones', *The Guardian*, 30 October [Online]. Available at: <https://www.theguardian.com/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance> (Accessed 17 April 2018).

Greenberg, A. (2017) 'The Silk Road creator's life sentence actually boosted dark web drug sales', *Wired*, 23 May. Available At: <https://www.wired.com/2017/05/silk-road-creators-life-sentence-actually-boosted-dark-web-drug-sales/> (Accessed: 20 March 2018).

Guzel, E. and Baban, E. (2016) *Digital Surveillance and Social Media*. USA: Create Space Independent Publishing Platform.

Hamill, J. (2013) 'Number of Cops Abusing Police National Computer Access on the Rise', *The Register*, [Online]. Available at: https://www.theregister.co.uk/2013/06/18/dozens_of_london_cops_investigated_for_misusing_controversial_police_database/ (Accessed: 20 February 2017).

Heaven, D. (2017) 'Abandon privacy online', *New Scientist*, 235(3133), pp. 31-32.

Kietzmann, J., Hermkens, K., McCarthy, I. and Silvestre, B. (2011) 'Social media? Get serious! Understanding the functional building blocks of social media', *Science Direct*, 54, pp. 241-251.

Lips, A. (2018) 'From chat rooms to snapchat: The history of social media', *Social Media Week*, 22 January [Online]. Available at: <https://socialmediaweek.org/blog/2018/01/chat-rooms-snapchat-history-social-media/> (Accessed 10 February 2018).

Mateescu, A., Brunton, D., Rosenblat, A., Patton, D., Gold, Z., and Boyd, D. (2015) 'Social media surveillance and law enforcement', *Data and Civil Rights: A New Era of Policing and Justice*, 27 October [Online]. Available at: http://www.datacivilrights.org/pubs/2015-1027/Social_Media_Surveillance_and_Law_Enforcement.pdf (Accessed: 19 Jan 2017).

Miles M.B., and Huberman A.M. (1994) *Qualitative data analysis: An expanded sourcebook*. Thousand Oaks, CA: SAGE Publications Inc.

Morgans, J. (2017) *Vice*. Available at: https://www.vice.com/en_us/article/vv5jkb/the-secret-ways-social-media-is-built-for-addiction (Accessed: 9 March 2018).

Nineteen Eighty-Four (1984) Directed by Michael Radford [Film]. London: MGM Films

Roufa, T. (2016b) 'Technologies that are changing the way police do business', *The Balance*, 8 October [Online]. Available At: <https://www.thebalance.com/technologies-that-are-changing-the-way-police-do-business-974549> (Accessed: 19 January 2017).

Sampson, F. (2017) 'Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings', *The Police Journal, Theory Practice and Principles*, 90(1), pp.55-69. [Online] Available At: <https://journals.sagepub.com/doi/pdf/10.1177/0032258X16671031> (Accessed: 23 March 2019).

Shade, L. and Singh, R. (2016) 'Honestly, we are not spying on your kids: School surveillance of young people's social media', *Social Media and Society*, pp. 1-12.

Scaife, L. (2015) *Handbook of Social Media and the Law*. New York: Routledge

Soat, M. (2015) 'Social media triggers a dopamine high', *Marketing News*, November [Online]. Available at: <https://www.ama.org/publications/MarketingNews/Pages/feeding-the-addiction.aspx> (Accessed: 20 January 2018).

Sottek, T.C. and Kopfstein, J. (2013) 'Everything you need to know about PRISM', *The Verge*, 17 July [Online]. Available at: <https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet> (Accessed: 20 March 2018).

Stephen, C. (2015) *The gamification of social media*. Available at: <https://www.meltwater.com/uk/blog/the-gamification-of-social-media> (Accessed: 19 May 2017).

Surette, R. (2016) 'How social media is changing the way people commit crimes and police fight them', *LSE USCentre*, 28 January. Available at: <http://bit.ly/1KcPPCt/> (Accessed: 23 September 2016).

Tait, M. (2015) 'College campuses are the new test facilities for emerging technology', *Techcrunch*. 12 December. Available at: <https://techcrunch.com/2015/12/12/college-campuses-are-the-new-test-facilities-for-emerging-technology/> (Accessed 12 March 2018).

The Economist Intelligence Unit (2008) *The future of higher education: How technology will shape learning* [Online]. Available at: <https://files.eric.ed.gov/fulltext/ED505103.pdf> (Accessed 15 March 2018).

Totter, A. (2010) Letter to colleges, 26 August.

Travis, E. (2017) 'Facebook isn't free: Its making billions from you', *Conversation Hub*. May. Available at: <https://conversion-hub.com/blog/internet-marketing-trends/facebook-isnt-free-making-billions/> (Accessed: 11 February 2018).

Trottier, D. (2015b) 'Coming to terms with social media monitoring: Uptake and early assessment', *Crime Media Culture*, 11(3), pp. 317-333.

Tunncliffe, I. and Tatham, S. (2017) *Social media the virtual ground: Can we hold it?* [Online]. Available at: <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1349> (Accessed: 4 February 2018).

Turel, O., Brevers, D. and Bechara, A. (2018) 'Time distortion when users at-risk for social media addiction engage in non-social media tasks', *Journal of Psychiatric Research*, 97, pp. 84-88.

Appendices

Appendix A – Focus Group Plan

Appendix B – Focus Group Information Sheet

Appendix C – Focus Group Consent Form

Appendix D – Final Draft Open Source Survey

Appendix E – Ethics Review Check List

Appendix F – Ethics Committee Compliance Letter

Appendix F – Initial time line for the project

Appendix G – Focus Group Coding

Appendix H – Survey Results

Appendix A

Focus Group Plan

1. Ensure room is set up appropriately, name cards, water and refreshments
2. Handouts for all participants, information sheet, consent forms, paper-based survey
3. Introductions
4. Read through information sheet and request consent forms to be signed.

First Session: Survey Related Discussion Questions: **Please complete the survey provided**

50 minutes to complete the survey and discuss the following:

1. **Having completed the survey what are your first thoughts about its structure and contents?**
2. **The survey is intended to gain an understanding of how officers are using Social Media & Open Source Platforms in a day to day policing context. Do you think there are any other questions that could/should be asked?**

Second session: Focus Group Questions:

30 minutes to discuss the following:

1. **In your experience do social media surveillance practices by the police officers take place.**
2. **In your experience discuss whether social media surveillance undermines current procedural protocols and legislative guidance?**
3. **Does the Metropolitan Police Service have sufficient procedural robustness around police social media surveillance and does the current MPS policy provide enough guidance?**
4. **Is there anything else anyone would like to add in relation to police use of social media for surveillance purposes?**

Appendix B

Focus Group Discussion Information Sheet



Title: Can I follow you? Social Media Surveillance and Policing Dilemmas

Welcome

Good morning and welcome to our session. Thank you for taking the time to join us to talk about the use of Open Source and Social Media in every day Policing. My name is Liam Cahill and assisting me is Paul Farmery. I am a Post Graduate student at Canterbury Christ Church University and currently studying for my MSc in Policing by Research. My assistant is from the Horizon Team in the Open Source Unit.

Background

In the last five – seven years, there has been a global shift in the way that police services communicate with the public. In part, this is due to advancements in technology, with 80% of the adult population having access to a mobile device, coupled with the introduction of social media and fundamental changes in the way society communicates with each other and the world around them.

Police communications have had to embrace these changes to ensure that they have a presence in this complex digital space and are increasingly looking to Social Media to support their everyday work from finding missing persons to investigating crime. However, these changes continue to be rapid, arguably impacting every area of policing business, but have the police and other investigative agencies truly considered the implications of using these platforms in the trade-off between security, privacy and organisational legitimacy?

The Metropolitan Police Service arguably has the largest Social Media presence of any Police Service/Force in the world. With this comes important challenges around training, technology, policy, understanding of relevant legislation and ensuring its ethical use by police officers.

Each of you works on a borough as the SPOC or lead for Social Media and you have been invited here today as you have a working knowledge of the benefits and drawbacks of social media in a policing context. You have the front-line experience of how the MPS is managing and engaging with Social Media day-to-day.

Through your positions, you may have some critical reflections around the way Social Media is being utilised by officers.

Useful Definitions

To assist you I have included the following key definitions.

Open Source Information refers to publicly available information, which any member of the public could obtain by request or observation.

In the context of this survey, Open Source includes any information that can be obtained by accessing the internet, such as social media, books, journals, TV and radio broadcasts

Online Investigation or Open Source Research is the collection, evaluation and analysis of materials from sources online available to the public, whether on payment or otherwise, to use as intelligence or as evidence within investigations.

Social Media is included in **Online Investigation (Open Source)** and refers to platforms where users generate and share content either openly or upon request. Examples of these platforms include Twitter and Facebook.

What will you be required to do?

The first part of the focus group is to ask you to complete a survey that we intend to distribute across the MPS in the coming weeks. We would like you to answer the questions and then discuss several areas of the survey. This should take approximately 50 minutes.

We'll take a short 10-minute break

We'll then come back for the second half of the discussion which will centre around the use of Social Media and policing. This should take approximately 30 minutes.

Ground Rules

Please ensure all mobile devices are on silent mode before we start.

It is important to remember that there are no wrong answers and please keep in mind that I am just as interested in negative comments as positive comments, and at times the negative comments are the most helpful.

There is no rank in these focus groups and we would ask you to address each other on a first name basis.

I'm tape recording the session because I don't want to miss any of your comments. People often say very helpful things in these interviews and sadly I can't write fast enough to accurately record everything.

My role as moderator is to encourage an open interview in relation to the key subject areas of Social Media surveillance.

To participate in this research

To participate in this focus group, you must work for the MPS either as an officer, PCSO, or member of staff and be involved in the borough maintenance or support of Social Media.

Procedures

Please use the cards in front of you to put your first names on. There are no wrong answers but rather differing points of view.

Please feel free to share your point of view even if it differs from what others have said. Keep in mind that we're just as interested in negative comments as positive comments, and at times the negative comments are the most helpful.

You have all been given a feedback sheet. I would ask you to put your first name on the top and if you have any thoughts or notes you wish to make throughout the discussion please do so and we will collect these in at the end of the discussion.

My role as moderator will be to guide the discussion. Talk to each other.

Feedback and Dissemination of results

The results of the research will be used by the Open Source Unit (SCO36) to improve the way that the MPS engages with Open Source platforms and consider whether officers have the right technology to safely utilise these resources. It will also be used to advise on policy improvements to support these endeavours.

The research will also be published through Canterbury Christ Church University upon completion and submitted to the College of Policing for the continued improvement of policing nationally. This focus group will be pivotal in ensuring that the survey is ready for distribution and the valuable discussions you have will be used in the research to support recommendations for the future.

If you would like to be notified when the research is complete and how to obtain a copy of the results please notify the interviewer.

Anonymity and Confidentiality

All data and personal information will be stored securely and anonymously within CCCU premises in accordance with the Data Protection Act 1998 and the University's own data and storage guidance for a period of five years after the degree has been awarded. Data can only be accessed by Liam Cahill, supervisors, examiners and auditors of Canterbury Christ Church University. After completion of the study, all data will be made anonymous (i.e. all personal information associated with the data will be removed).

We will be on a first name basis during this discussion and we won't use any of your names in subsequent reports. While I can assure you of complete confidentiality and any details recorded will be secured by the researcher and not

for public/organisational consumption I cannot guard against participants in the focus groups discussing details of what takes place or who was present.

Please bare this in mind when agreeing to take part.

Deciding whether to participate

If you have any questions or concerns about the nature, procedures or requirements for participation do not hesitate to contact me. Should you decide to participate, you will be free to withdraw at any time without having to give a reason.

Any questions?

Please contact Liam Cahill on l.cahill441@canterbury.ac.uk or my supervisory, Martin Wright p.wright537@canterbury.ac.uk

Appendix C



CONSENT FORM

Title of Project: Can I follow you? Social Media Surveillance and Policing Dilemmas

Name of Researcher: Liam Cahill

Contact details:

Address:	Ealing Police Station 67-69 Uxbridge Road Ealing W5 5SJ
Tel:	07976 702 598
Email:	l.cahill441@canterbury.ac.uk

Please initial

box

1. I confirm that I have read and understand the information sheet for the above study and have had the opportunity to ask questions.
2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason.
3. I understand that any personal information that I provide to the researchers will be kept strictly confidential
4. I agree to the focus group being audio recorded
I agree take part in the above study.

_____ Name of Participant	_____ Date	_____ Signature
_____ Name of Person taking consent (if different from researcher)	_____ Date	_____ Signature
_____ Researcher	_____ Date	_____ Signature

Contact Details:
Researcher - Liam Cahill l.cahill@canterbury.ac.uk
Supervisor - Martin Wright p.wright537@canterbury.ac.uk

Copies: 1 for participant
1 for researcher

Appendix C



CONSENT FORM

Title of Project: Can I follow you? Social Media Surveillance and Policing Dilemmas

Name of Researcher: Liam Cahill

Contact details:

Address:	Ealing Police Station 67-69 Uxbridge Road Ealing W5 5SJ
Tel:	07976 702 598
Email:	l.cahill441@canterbury.ac.uk

Please initial

box

1. I confirm that I have read and understand the information sheet for the above study and have had the opportunity to ask questions.
2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason.
3. I understand that any personal information that I provide to the researchers will be kept strictly confidential
4. I agree to the focus group being audio recorded
I agree take part in the above study.

Name of Participant

Date

Signature

Name of Person taking consent
(if different from researcher)

Date

Signature

Researcher

Date

Signature

Contact Details:

Researcher - Liam Cahill l.cahill@canterbury.ac.uk

Supervisor - Martin Wright p.wright537@canterbury.ac.uk

Copies: 1 for participant
1 for researcher

Appendix D

Online Investigation (Open Source) staff survey Information Sheet

Introduction:

Online Investigation or Open Source research is an extremely valuable capability for the Police. It can be extremely useful in many investigations. However, to determine how Online Investigation (Open Source) is utilised within the MPS, we would like to understand how and when it is being used by you.

When we talk about Online Investigation or 'Open Source' in your work, we are referring to how you access and use the internet to identify the information you require.

Who is this survey for?

This survey is for anyone who uses Online Investigation (Open Source) for engagement, intelligence, research or evidence gathering. It includes the use of social media or any platform via the internet and should take no longer than 20 minutes to complete.

Purpose:

The information you provide in this survey will be used to determine whether the MPS has the best infrastructure, policies, procedures and safeguards for officers and the public. As the use of Online Investigation (Open Source) research, intelligence and evidence becomes more prevalent in day-to-day policing and the fight against crime, it is vital that the MPS provides its officers with the right tools to access and use it effectively and efficiently.

Definitions:

To assist you in the completion of this survey we have included the following key definitions.

Open Source Information refers to publicly available information, which any member of the public could obtain by request or observation.

In the context of this survey, Open Source includes any information that can be obtained by accessing the internet, such as social media, books, journals, TV and radio broadcasts

Online Investigation or Open Source Research is the collection, evaluation and analysis of materials from sources online available to the public, whether on payment or otherwise, to use as intelligence or as evidence within investigations.

Social Media is included in Online Investigation (Open Source) and refers to platforms where users generate and share content either openly or upon request. Examples of these platforms include Twitter and Facebook.

How your information will be used:

This survey is **anonymous**. While some demographics have been requested as part of the survey, this is to assist in statistical analysis and is not for identification purposes.

The details you provide will be vital to the Met Intel Horizons Team who are evaluating the current use of Online Investigation (Open Source) research in order to identify potential improvements for the MPS. Additionally, Liam Cahill will be using the data as part of his masters degree in Policing by Research at Canterbury Christ Church University where he is researching police use of social media.

Federation advice has been sought in relation to this survey and has been validated by Paul Clarke from HQ Strategy & Governance for the MPS. The MPS wishes participants to be open and honest when completing this survey for the ongoing improvement and development of the organisation.

Further information:

For further information on this survey, how the information will be used or the research being conducted, please contact Liam Cahill on l.cahill441@canterbury.ac.uk, his supervisor Martin

PLEASE REMEMBER - THIS SURVEY IS COMPLETELY ANONYMOUS

1. To what level are you trained in Online Investigation (Open Source)?

- Level 1 (Not specifically trained)
- Level 2 (Core Open Source Investigation/Research)
- Level 3 (Advanced Open Source Investigation/Research)
- Level 4 (Network Investigations)
- Level 5 (Undercover Officer online, Covert Internet Investigator)

(NEXT QUESTION)

2. Have you received any training in the use of social media? If yes, please tick all that apply.

- Trained by the Department of Media and Communications (DMC)
- Trained by a Borough SPOC
- Self-taught
- No training received
- Other (please explain): **(FREE TEXT – Max 100 words?)**

(NEXT QUESTION)

3. Do you use/have access to an Official MPS Social Media Account (such as @metpoliceuk etc.)?

- Yes
- No

(NEXT QUESTION)

4. Approximately how often do you use Online Investigation (Open Source) research in your work?

- Very frequently (several times a day)
- Frequently (1-2 times a day)
- Occasionally (2-3 times a week)
- Rarely (2-3 times a month)
- Very rarely (once a month or less)
- Other (please explain): **(FREE TEXT – Max 250 words?)**

(NEXT QUESTION)

5. If you are happy to do so, please briefly describe how you generally use/have used Online Investigation (Open Source) research in your work.

(FREE TEXT – Max 1000 words?)

(NEXT QUESTION)

6. Are you aware that the Open Source Unit at Cobalt Square is able to conduct Online Investigation (Open Source) research on your behalf?

Yes
No

(NEXT QUESTION)

7. How have you conducted Online Investigation (Open Source) research? Please tick all that apply.

Request submitted to Open Source Unit
Request submitted to LIT
Request submitted via CrimInt
Used a Aware terminal (MPS desktop computer / tablet device etc.)
Used a Covert terminal (standalone, not overtly linked to the MPS)
Used my personal, non-work related device (your own phone/tablet etc.)
(sub question below)
Other (please explain): (FREE TEXT – Max 1000 words?)

(NEXT QUESTION)

7.1 (If Personal device selected as a response to Q7)

For what reason(s) did you use the personal device to conduct Online Investigation (Open Source) research? Please tick all that apply.

Missing person enquiries
Criminal investigation
Domestic Incident
Civil Dispute
Road Traffic Collision
Critical Incident
Finding information for a member of the public
To give directions to a member of the public
To access information/a website that was blocked by Aware
To access information about a person/suspect/wanted offender
To update an MPS Social Media Platform
Monitoring of a suspected offender's Social Media account
Other: (FREE TEXT – Max 1000 words?)

If possible, please provide further details of the incident/occasion to help us understand why you used your own device.

(FREE TEXT – Max 1000 words?)

(NEXT QUESTION)

8. Are there any specific occasions/reasons for why you have not used the services of the Open Source Unit? If yes, please tick all that apply.

Research could be carried out via own personal device
Research could be carried out via Aware
Research could be carried out via a standalone (incl. via LIT, a colleague)
Didn't or don't know the remit for the Open Source Unit
Didn't or don't know how to contact the Open Source Unit
Didn't or don't know that the Open Source Unit is open 24/7
My request to the Open Source Unit was refused
Too time consuming to request research through the Open Source Unit
Not applicable
Other (please explain): (FREE TEXT – Max 1000 words?)

(NEXT QUESTION)

9. Have you ever used your personal social media account (Facebook etc.) to conduct Online Investigation (Open Source) research?

Yes Please explain: (FREE TEXT – Max 1000 words?)

No

(NEXT QUESTION)

10. Have you used a false persona (assumed identity to mask your own) to conduct Online Investigation (Open Source) searches/research?

Yes (sub question below)

No

(NEXT QUESTION)

10.1 (If yes to Q10)

What device(s) have you used when using a false persona? Please tick all that apply.

Personal, non-work related device (your own phone/tablet etc.)

Aware terminal (MPS desktop computer / tablet device etc.)

Covert terminal (standalone machine, not overtly linked to the MPS)

(NEXT QUESTION)

11. This question is only applicable if you have ever used a personal, non-work related device/account for Policing purposes.

Have you ever experienced any unwanted / malicious messages or calls etc. as a result of using your own device and/or social media account for Police work?

Yes Please explain: (FREE TEXT – Max 2500 words?)

No

Not applicable

(NEXT QUESTION)

12. Would you benefit from easier access to the internet as an investigative tool?

Yes (sub question below)

No

12.1 (If yes to Q12)

Please tell us more about how exactly you would benefit from better Internet access.

(FREE TEXT – Max 500 words?)

(NEXT QUESTION)

13. Would you benefit from additional Online Investigation (Open Source) training?

Yes (sub question below)

No

13.1. (If yes to Q13)

Please tell us more about how exactly you would benefit from additional training.

(FREE TEXT – Max 500 words?)

(NEXT QUESTION)

14. Please use the space below to make any comments or suggestions for improvement in regards to Online Investigation (Open Source) in the MPS?

(FREE TEXT – Max 1000 words?)

(NEXT QUESTION)

15. To help us better understand your responses please tell us what your current rank/grade is.

- Band E
- Band D
- Band C
- PC/DC
- PS/DS
- Insp/DI
- Prefer not to say

Other - Please enter your rank/grade: (FREE TEXT)

(NEXT QUESTION)

16. Please state your length of service.

- 0 – 2
- 2 – 5
- 5 – 10
- 10 – 15
- 15 – 20
- 20 – 25
- 25 – 30
- 30+ years

(NEXT QUESTION)

17. Please select your age group.

- 18 – 24
- 25 – 34
- 35 – 44
- 45 – 54
- 55 and over
- Prefer not to say

(NEXT QUESTION)

There are just a few more questions which, if completed, would be of great benefit to Liam Cahill and his ongoing work. We'd be most grateful if you could spend just a little more time in answering these last questions.

If you're happy to proceed, please click NEXT.

If you would like to end this survey here, please click FINISH.

(NEXT) – TO FINAL SET OF QUESTIONS BELOW

(FINISH) – TO FINAL SCREEN

Thanks for your time. It really is very much appreciated. If you have any questions or would like to engage with us in regards to Online Investigation (Open Source) in the MPS, we would be delighted to hear from you. Please contact the Met Intel Horizons Team via email - **Met Intel Mailbox - Horizons Team**.

If you are interested in the research being conducted by PS Liam Cahill around police use of social media you can contact him on l.cahill441@canterbury.ac.uk

(CLOSE)

Thank you for completing the survey so far. The following questions are designed to help provide an insight into levels of knowledge around legislation and policy that affect the use of Social Media, together with your professional views around privacy. By answering the following questions it will support future training and policy development within the MPS.

Once again please let me remind you that all of your answers are **anonymous** and that there is no right or wrong answer.

(NEXT)

1. Does the Regulation of Investigatory Powers Act (RIPA 2000) impact the way in which police obtain Online Investigation (Open Source) intelligence?

- Yes (pop up) Please briefly explain why **(FREE TEXT – Max 1000 words?)**
No (pop up) Please briefly explain why **(FREE TEXT – Max 1000 words?)**
Don't know

(NEXT QUESTION)

2. Does MPS Policy on the covert use of Social Media and Open Source Intelligence impact your use of these platforms?

(FREE TEXT – Max 1000 words?)

- Yes (pop up) Please briefly explain why **(FREE TEXT – Max 1000 words?)**
No (pop up) Please briefly explain why **(FREE TEXT – Max 1000 words?)**
Don't know

(NEXT QUESTION)

3. Does the College of Policing 'Code of Ethics' apply to the use of open source engagement and research?

- Yes (pop up) Please briefly explain why **(FREE TEXT – Max 1000 words?)**
No (pop up) Please briefly explain why **(FREE TEXT – Max 1000 words?)**
Don't know

(NEXT QUESTION)

4. The privacy/security debate is an important one for society and the legitimacy of the police. Do you think the police should automatically have the right to view open source information regardless of how personal, for policing purposes?

- Yes (pop up) Please briefly explain why **(FREE TEXT – Max 1000 words?)**

No (pop up) Please briefly explain why (**FREE TEXT – Max 1000 words?**)
Don't know

(FINISH) – TO FINAL SCREEN

Thanks for your time. It really is very much appreciated. If you have any questions or would like to engage with us in regard to Online Investigation (Open Source) in the MPS, we would be delighted to hear from you. Please contact the Met Intel Horizons Team via email - **Met Intel Mailbox - Horizons Team**.

If you are interested in the research being conducted by PS Liam Cahill around police use of social media you can contact him on l.cahill441@canterbury.ac.uk

(CLOSE)

Appendix E



For Research Office Use
Checklist No:
Date
Received:

PROPORTIONATE ETHICAL REVIEW ETHICS REVIEW CHECKLIST

Your application **must** comprise the following documents (please tick the boxes below to indicate that they are attached):

Ethics Review Checklist

Risk Assessment Form x3

Copies of any documents to be used in the study:

Questionnaire

Introductory letter(s)

Participant Information Sheet(s)

Consent Form(s)

Data Collection Instruments

Interview Questions

Focus Group Guidelines

Other (please give details)

For Research Office Use
Checklist No:
Date
Received:

PROPORTIONATE ETHICAL REVIEW

ETHICS REVIEW CHECKLIST

Sections A and B of this checklist must be completed for every research or knowledge transfer project that involves human or animal¹ participants. These sections serve as a toolkit that will identify whether a full application for ethics approval needs to be submitted.

If the toolkit shows that there is **no need for a full ethical review**, Sections D, E and F should be completed and the checklist emailed to red.resgov@canterbury.ac.uk as described in Section C.

If the toolkit shows that **a full application is required**, this checklist should be set aside and an *Application for Faculty Research Ethics Committee Approval Form* - or an appropriate external application form - should be completed and submitted. **There is no need to complete both documents.**

Before completing this checklist, please refer to *Ethics Policy for Research Involving Human Participants* and the *Code of Practice for the Use of Sentient Animals in Research and Teaching* on the University Research website.

The principal researcher/project leader (or, where the principal researcher/project leader is a student, their supervisor) is responsible for exercising appropriate professional judgement in this review.

N.B. This checklist must be completed – and any resulting follow-up action taken - before potential participants are approached to take part in any study.

Type of Project - please mark (x) as appropriate			
Research	<input checked="" type="checkbox"/>	Knowledge Exchange	<input type="checkbox"/>

Section A: Applicant Details

A1. Name of applicant:	Liam Cahill
A2. Status (please underline):	Postgraduate Student
A3. Email address:	l.cahill441@canterbury.ac.uk
A4. Contact address:	119A The Greenway Uxbridge UB8 2PR
A5. Telephone number	07976 702 598

¹ Sentient animals, generally all vertebrates and certain invertebrates such as cephalopods and crustaceans

² Checklists for Undergraduates should be retained within the academic department concerned

Section B: Ethics Checklist

Please answer each question by marking (X) in the appropriate box:

		Yes	No
1.	Does the study involve participants who are particularly <u>vulnerable</u> or unable to give informed consent (e.g. children, people with learning disabilities), or in unequal relationships (e.g. people in prison, your own staff or students)?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.	Will the study require the co-operation of a gatekeeper for initial access to any <u>vulnerable</u> groups or individuals to be recruited (e.g. students at school, members of self-help groups, residents of nursing home)?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.	Will it be necessary for participants to take part in the study without usual informed consent procedures having been implemented in advance (e.g. covert observation, certain ethnographic studies)?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.	Will the study use deliberate deception (this does not include randomly assigning participants to groups in an experimental design)?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.	Will the study involve discussion of, or collection of information on, topics of a sensitive nature (e.g. sexual activity, drug use) <u>personal to the participants</u> ?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.	Are drugs, placebos or other substances (e.g. food substances, vitamins) to be administered to human or animal participants?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
7.	Does the study involve invasive or intrusive procedures such as blood taking or muscle biopsy from human or animal participants?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
8.	Is physiological stress, pain, or more than mild discomfort to humans or animals likely to result from the study?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9.	Could the study induce psychological stress or anxiety or cause harm or negative consequences in humans (including the researcher) or animals beyond the risks encountered in normal life?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.	Will the study involve interaction with animals? (If you are simply observing them - e.g. in a zoo or in their natural habitat - without having any contact at all, you can answer "No")	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.	Will the study involve prolonged or repetitive testing?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
12.	Will financial inducements (other than reasonable expenses and compensation for time) be offered to participants?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
13.	Is the study a survey that involves University-wide recruitment of students from Canterbury Christ Church University?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
14.	Will the study involve recruitment of adult participants (aged 16 and over) who are unable to make decisions for themselves, i.e. lack capacity, and come under the jurisdiction of the Mental Capacity Act (2005)?	<input type="checkbox"/>	<input type="checkbox"/>
15.	Will the study involve recruitment of participants (excluding staff) through the NHS?	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Now please assess outcomes and actions by referring to Section C 

Section C: How to Proceed

C1. If you have answered ‘NO’ to *all* the questions in Section B, you should complete Sections D–F as appropriate and email the completed checklist to red.resgov@canterbury.ac.uk. **That is all you need to do.** **Once your application is assessed and if it is given approval you will receive a letter confirming compliance with University Research Governance procedures.**

[*Master’s students should retain copies of the form and letter; the letter should be bound into their research report or dissertation. Work that is submitted without this document will be returned un-assessed.*]

C2. If you have answered ‘YES’ to *any* of the questions in Section B, you will need to describe more fully how you plan to deal with the ethical issues raised by your project. This does not mean that you cannot do the study, only that your proposal will need to be approved by a Research Ethics Committee. **Depending upon which questions you answered ‘YES’ to, you should proceed as follows**

(a) If you answered ‘YES’ to any of *questions 1 – 12 ONLY* (i.e. not questions 13,14 or 15), you will have to submit an application to your Faculty Research Ethics Committee (FREC) using your Faculty’s version of the *Application for Faculty Research Ethics Committee Approval Form*. This should be submitted as directed on the form. The *Application for Faculty Research Ethics Committee Approval Form* can be obtained from the Research Ethics pages of the Research and Enterprise Development Centre on the University web site.

(b) If you answered ‘YES’ to *question 13* you have two options:

(i) If you answered ‘YES’ to *question 13 ONLY* you must send copies of this checklist to the Student Survey Unit. Subject to their approval you may then proceed as at C1 above.

(ii) If you answered ‘YES’ to *question 13 PLUS any other of questions 1 – 12*, you must proceed as at C2(b)(i) above and then submit an application to your Faculty Research Ethics Committee (FREC) as at C2(a).

(c) If you answered ‘YES’ to *question 14* you do not need to submit an application to your Faculty Research Ethics Committee. **INSTEAD**, you **must** submit an application to the appropriate external NHS or Social Care Research Ethics Committee [see C2(d) below].

(d) If you answered ‘YES’ to *question 15* you do not need to submit an application to your Faculty Research Ethics Committee. **INSTEAD**, you must submit an application to the appropriate external NHS or Social Care Research Ethics Committee (REC), *after* your proposal has received a satisfactory Peer Review (see *Research Governance Handbook*). Applications to an NHS or Social Care REC **must** be signed by the appropriate Faculty Director of Research or other authorised Faculty signatory before they are submitted.

IMPORTANT

Please note that it is your responsibility in the conduct of your study to follow the policies and procedures set out in the University’s Research Ethics website, and any relevant academic or professional guidelines. This includes providing appropriate information sheets and consent forms, and ensuring confidentiality in the storage and use of data. Any significant change in the question, design or conduct over the course of the study should be notified to the **Faculty and/or other Research Ethics Committee** that received your original proposal. Depending on the nature of the changes, a new application for ethics approval may be required.

Section D: Project Details

D1. Project title:	Can I follow you? Social media surveillance & policing dilemmas
D2. Start date of fieldwork	9 th October 2017
D3. End date of fieldwork	31 st January 2017
D4. Lay summary (max 300 words <i>which must include a brief description of the methodology to be used for gathering your data</i>)	<p>I will be researching how police officers use open source platforms such as Facebook and Twitter and do they routinely engage in social media surveillance whether authorised or otherwise through the use of these platforms.</p> <p>I will begin by running a series of focus groups with the Single Points of Contact (SPOC) for social media from each of the 32 London Boroughs before deploying a survey across the MPS.</p> <p>This research is supported by the Metropolitan Police Service and College of Policing and is intended to demonstrate a new theoretical understanding of social media surveillance in a policing context. While establishing whether there is an organisational need to improve procedural protocols and legislative guidance to ensure that the police are not conducting, unauthorised, non-auditable surveillance on digital society. In a wider context I will consider how the findings impact the security/privacy debate.</p>

Section E1: For Students Only

E1. Module name and number or course and Department:	MSc by Research
E2. Name of Supervisor or module leader	Dr Martin Wright
E3. Email address of Supervisor or Module leader	p.wright537@canterbury.ac.uk
E4. Contact address:	Canterbury Christ Church University School of Law, Criminal Justice and Computing Canterbury CT1 1QU

Section E2: For Supervisors

Please tick the appropriate boxes. The study should not begin until all boxes are ticked:

<p>The student has read the relevant documentation relating to the University's Research Governance, available on the University web pages at:</p> <p>https://cccu.canterbury.ac.uk/research-and-enterprise-development-centre/research-governance-and-ethics/research-governance-and-ethics.aspx</p>	<div style="border: 1px solid black; width: 40px; height: 40px; margin: 0 auto; display: flex; align-items: center; justify-content: center;">X</div>
---	---

The topic merits further investigation	X
The student has the skills to carry out the study	X
The participant information sheet or leaflet is appropriate	X
The procedures for recruitment and obtaining informed consent are appropriate	X
If a Disclosure & Barring Service (DBS) check is required, this has been carried out	

Comments from supervisor:

The study enjoys the support of the College of Policing and the Metropolitan Police and is considered to be of importance. I wholly support this research.

Section F: Declaration

- I certify that the information in this form is accurate to the best of my knowledge and belief and I take full responsibility for it.
- I certify that a risk assessment for this study has been carried out in compliance with the University's Health and Safety policy.
- I certify that any required Disclosure & Barring Service (DBS) check has been carried out.
- I undertake to carry out this project under the terms specified in the Canterbury Christ Church University Research Governance Handbook.
- I undertake to inform the relevant Faculty Research Ethics Committee of any significant change in the question, design or conduct of the study over the course of the study. I understand that such changes may require a new application for ethics approval.
- I undertake to inform the RKE Co-ordinator at red.resgov@canterbury.ac.uk in the Research and Enterprise Development Centre when the proposed study has been completed.
- I am aware of my responsibility to comply with the requirements of the law and appropriate University guidelines relating to the security and confidentiality of participant or other personal data.
- I understand that project records/data may be subject to inspection for audit purposes if required in future and that project records should be kept securely for five years or other specified period.
- I understand that the personal data about me contained in this application will be held by the Research and Enterprise Development Centre and that this will be managed according to the principles established in the Data Protection Act.

As the Principal Investigator for this study, I confirm that this application has been shared with all other members of the study team	(please tick) ✓
--	--------------------

Principal Investigator	Supervisor or module leader (as appropriate)
Name: Liam Cahill	Name: Dr Martin Wright
Date: 11.10.2017	Date: 11.10.2017

Section G: Submission

This form should be sent as an attachment to a covering email, to red.resgov@canterbury.ac.uk

N.B. YOU MUST include copies of the Participant Information Sheet and Consent Form that you will be using in your study (Model versions on which to base these

are appended below for your convenience). Also copies of any data gathering tools such as questionnaires, and a **COMPLETED RISK ASSESSMENT FORM**.

All Participant Information Sheets, Consent Forms and Risk Assessments have been supplied separately to this document.

Appendix F



18th December 2017
17/SAS/04F

Ref:

Liam Cahill
c/o School of Law, Criminal Justice and Computing
Faculty of Social & Applied Science

Dear Liam

Confirmation of ethics compliance for your study “*Can I follow you? Social media surveillance & policing dilemmas*”

Your application complies fully with the requirements for full ethical review as set out in this University’s Research Ethics and Governance Procedures.

In confirming compliance for your study, I must remind you that it is your responsibility to follow, as appropriate, the policies and procedures set out in the *Research Governance Framework* (<http://www.canterbury.ac.uk/research-and-consultancy/governance-and-ethics/governance-and-ethics.aspx>) and any relevant academic or professional guidelines. This includes providing, if appropriate, information sheets and consent forms, and ensuring confidentiality in the storage and use of data. Any significant change in the question, design or conduct of the study over its course should be notified to the **Ethics Chair of Social & Applied Sciences**, and may require a new application for ethics approval. [It is a condition of compliance that you must inform me once your research has been completed.](#)

Wishing you every success with your research.

Yours sincerely

Carol Clewlow
(On behalf on Dr Dennis Nigbur)

Carol Clewlow
RKE Co-Ordinator
Tel: +44 (0)1227 922893 (direct line)
Email: red.resgov@canterbury.ac.uk

Appendix F – Initial time line for the project **Research Timeline**

Activity	Questions/Issues	Est. Time	Deadline	Notes	Completed
Research Questions	Consider complications with MPS		Oct 16	MPS HQ and Strategy Engaged	Completed
Identification of reading material	Lack of relevant literature	ongoing	ongoing	Continue reading throughout research	Completed
Identification of reading for methodology	-	2 months	March 17		Completed
Literature Review First Draft	Submitted	2 weeks	April 17	Issues raised – see feedback	Completed
Literature Review Rewrite	Not enough focus on surveillance theory	2 Weeks	April 17		Completed
Research Questions Drafted		4 Weeks	Jan 17	Panel Approved	Completed
Research proposal Written		4 Weeks	Jan 17	Panel Approved	Completed
Intended Methodology	First Draft	1 Week	Jun 17		Completed
Methodology/Method Design	Final Submission	1 Week	Jun 17		Completed
Survey Drafted					Completed
Focus Group Planned	Protecting anonymity of participants is paramount discuss with tutor.	2 months	Sep 17	Methods considered/Risk Assessment Completed.	Completed
Focus Groups Arranged		2 weeks	Sep 17	Participants identified during planning – All e-mailed directly	Completed
Focus Group Conducted/Survey Piloted	Changes to survey identified from focus group pilot	3 dates booked	Oct 17	Conducted over 3 sessions at NSY	Completed
Survey Amendments		4 weeks	Nov 17		
Distribute Survey		6 Weeks	Jan - Feb 18	Distributed using the MPS Intranet, waited till Jan due to Christmas holidays	Completed
Transcribe Focus Groups	-	2 months	Dec 17	-	Completed
Focus Group Analysis		1 month	Jan 18		Completed
Survey Analysis	-	2 months	April 18	-	Completed
Delay in completion due to moving house, changing job and birth of son	Extension Granted	-	-	Extension Granted	-
Dissertation Write Up		5 months	Mar 19		Completed

Appendix G – Focus Group Analysis – Figure 4.

Thematic Coding	Themes	Focus Group 1	Focus Group 2	Focus Group 3
What are the phenomena of concern being mentioned?		The phenomena being discussed was whether police personnel who have not received trained are utilising open source information obtained through personal social media accounts and devices for intelligence and evidence gathering and whether that practice constitutes a form of surveillance.		
Who are the persons involved?	Police Personnel	<p>Participant: 'I think the wanted offenders' unit use [social media to locate individuals] ... We have had jobs come through where a wanted person whose checked into this pub and needs officers to do an arrest enquiry.'</p>	<p>Participant: 'The one thing ... it does get used for by some officers on social media is when you've got high risk missing people, you'll search their name and see if you can get any information on them.' [Focus agrees because they are high risk]</p>	<p>Facilitator: 'Has anyone else been asked to look at other peoples' social media pages to gather intelligence?'</p> <p>Participant: 'I get it quite a lot, a Duty Inspector asked me to hack a person's Facebook account... as they were a missing person.'</p>
		<p>Participant: '[using of social media for intelligence purposes] It does happen.'</p> <p>Facilitator: 'Do you mean police officers are doing it?'</p> <p>Participant: 'Yes.'</p>	<p>Participant: 'I wonder if it could be generational, we've all had social media but we have all had [training] in the job. Where as the ones that are coming through brand new now have all got their own ward accounts. If something comes up and they want to look at someone, they might instantly think i'll go on Twitter or i'll go on Facebook.' [group agrees]</p> <p>Participant: 'And they wouldn't even seem out of place.'</p>	<p>Participant: 'The Twitter password was given out long before I got there. I know what I am doing ... but you have people compromising our Twitter and potentially our Facebook because they have logins and then track other people's accounts, which if that came out in the press...'</p>
		-	-	<p>Participant: 'A Duty Inspector asked me to hack into a person's Facebook.'</p>
When is the phenomena taking place? How long does it take and when does it occur?	Any Time & Place	<p>Participant: '[The use of social media for investigation purposes]. We see it all the time, its very very common.'</p>	<p>Participant: 'The one thing ... it does get used for by some officers on social media is when you've got high risk missing people.'</p>	<p>Participant: 'If it's 3 o'clock in the morning and the officer has a high risk missing child and they have a [social media] account, I expect there are officers you have done it.'</p>
How much/how Strong? – How often is the issue emphasised?	Getting the Job Done	<p>Facilitator: 'In terms of the survey does that draw out? I mean you guys have looked at it [and answered the questions], well I don't do that, I don't use my personal device or use [social media] for intelligence gathering purposes, but do the questions seek to find out if people are doing it?'</p> <p>Participant: 'It does happen regularly. We see it all the time, its very common and whether on YouTube or Facebook you seek the suspect. I mean it's very common.'</p>	<p>Participant: 'You know we are adults! If we can't do something one way we'll find another, we won't go back to mommy and say this isn't working give me access. It's time consuming, I wouldn't even know how to get in touch with the whole web marshal thing. I just ignore it, when I see that page, I close it and just go to the phone because it's there.'</p>	<p>Participant: 'We are in a massively changing world. It's changing far to fast for me to keep up with, which I accept, but is the job keeping up with it? Are the officers keeping up with it in order to get the job done legally to cover their backs.'</p>
	Don't Talk About It	-	<p>Facilitator: 'Are there any examples of people using social media for investigative purposes?'</p> <p>Participant: 'I know for a fact it happens.'</p> <p>Participant: 'You just don't talk about it.'</p>	-
What is the intention of the phenomena?	Necessity	<p>Participant: 'I think a lot of us are aware that we are not supposed to use our phones for this kind of research no matter how good our intentions are.'</p>	<p>Participant: 'I can't view videos on AWARE, so I have to use my phone to view the video via Instagram to see what it is because the public want a response from us. I need to see what it is so I can get back to them.'</p>	<p>Participant: 'If it's 3 o'clock in the morning and the officer has a high risk missing child and they have a [social media] account, I expect there are officers you have done it (conducted searches) from their own devices ... The argument becomes, yes I did it, but I would rather stand there in front of a disciplinary board and say I had a 14-year-old girl, high risk missing person who I was trying to locate ... than stand in front of a coroner's court [explaining why I didn't conduct the search].'</p> <p>Participant: 'You feel ... they can justify doing it for that reason, if I get caught, I get caught, I feel like I am doing it for the greater good.'</p>

Thematic Coding	Themes	Focus Group 1	Focus Group 2	Focus Group 3
What are the phenomena of concern being mentioned?	The phenomena being discussed was whether police personnel who have not received trained are utilising open source information obtained through personal social media accounts and devices for intelligence and evidence gathering and whether that practice constitutes a form of surveillance.			
Who are the persons involved?	Police Personnel	Participant: 'I think the wanted offenders' unit use [social media to locate individuals] ... We have had jobs come through where a wanted person whose checked into this pub and needs officers to do an arrest enquiry.'	Participant: 'The one thing ... it does get used for by some officers on social media is when you've got high risk missing people, you'll search their name and see if you can get any information on them.' [Focus agrees because they are high risk]	Facilitator: 'Has anyone else been asked to look at other peoples' social media pages to gather intelligence?' Participant: 'I get it quite a lot, a Duty Inspector asked me to hack a person's Facebook account... as they were a missing person.'
		Participant: '[using of social media for intelligence purposes] It does happen.' Facilitator: 'Do you mean police officers are doing it?' Participant: 'Yes.'	Participant: 'I wonder if it could be generational, we've all had social media but we have all had [training] in the job. Where as the ones that are coming through brand new now have all got their own ward accounts. If something comes up and they want to look at someone, they might instantly think i'll go on Twitter or i'll go on Facebook.' [group agrees] Participant: 'And they wouldn't even seem out of place.'	Participant: 'The Twitter password was given out long before I got there. I know what I am doing ... but you have people compromising our Twitter and potentially our Facebook because they have logins and then track other people's accounts, which if that came out in the press...'
		-	-	Participant: 'A Duty Inspector asked me to hack into a person's Facebook.'
When is the phenomena taking place? How long does it take and when does it occur?	Any Time & Place	Participant: '[The use of social media for investigation purposes]. We see it all the time, its very very common.	Participant: 'The one thing ... it does get used for by some officers on social media is when you've got high risk missing people.'	Participant: 'If it's 3 o'clock in the morning and the officer has a high risk missing child and they have a [social media] account, I expect there are officers you have done it.'
How much/how Strong? – How often is the issue emphasised?	Getting the Job Done	Facilitator: 'In terms of the survey does that draw out? I mean you guys have looked at it [and answered the questions], well I don't do that, I don't use my personal device or use [social media] for intelligence gathering purposes, but do the questions seek to find out if people are doing it?' Participant: 'It does happen regularly. We see it all the time, its very common and whether on YouTube or Facebook you seek the suspect. I mean it's very common.'	Participant: 'You know we are adults! If we can't do something one way we'll find another, we won't go back to mommy and say this isn't working give me access. It's time consuming, I wouldn't even know how to get in touch with the whole web marshal thing. I just ignore it, when I see that page, I close it and just go to the phone because it's there.'	Participant: 'We are in a massively changing world. It's changing far to fast for me to keep up with, which I accept, but is the job keeping up with it? Are the officers keeping up with it in order to get the job done legally to cover their backs.'
	Don't Talk About It	-	Facilitator: 'Are there any examples of people using social media for investigative purposes?' Participant: 'I know for a fact it happens.' Participant: 'You just don't talk about it.'	-
What is the intention of the phenomena?	Necessity	Participant: 'I think a lot of us are aware that we are not supposed to use our phones for this kind of research no matter how good our intentions are.'	Participant: 'I can't view videos on AWARE, so I have to use my phone to view the video via Instagram to see what it is because the public want a response from us. I need to see what it is so I can get back to them.'	Participant: 'If it's 3 o'clock in the morning and the officer has a high risk missing child and they have a [social media] account, I expect there are officers you have done it (conducted searches) from their own devices ... The argument becomes, yes I did it, but I would rather stand there in front of a disciplinary board and say I had a 14-year-old girl, high risk missing person who I was trying to locate ... than stand in front of a coroner's court [explaining why I didn't conduct the search].' Participant: 'You feel ... they can justify doing it for that reason, if I get caught, I get caught, I feel like I am doing it for the greater good.'

Thematic Coding	Themes	Focus Group 1	Focus Group 2	Focus Group 3
By which – Means/Tactics and strategies for achieving the aim. How are they doing it?	<i>Easy/Accessible/Covert</i>	Participant: 'I think a lot of us are aware that we are not supposed to use our phones for this kind of research no matter how good our intentions are.'	Participant: 'You could argue that the MPS is trying to say, you can't do this because they block sites like YouTube and certain aspects of Twitter. But it's not clear, for us we are investigators and if one avenue is blocked, we will find another one. [Group agree] I can't get it on Firefox, my phone will do it!' Facilitator: 'Do you think this is something that is happening regularly?' Participant: 'Oh yeah.' [Multiple members make agreeing sounds]	Participant: 'On Twitter for the last so many years we have been told to click on followers to see who is following us, it's a bit of a grey area with Facebook we quiet often get suspects being tagged on their own wanted appeals and we might click on them to see who they are. We have had people charged off a screenshot of facebook.'
	<i>False Persona</i>	Facilitator: 'How do you feel about false persona?' Participant: 'I think you would need some authority to do that.'	Facilitator: 'Level 2 open source training and above allows you to adopt a false persona to conduct online investigations, At level 3 you can befriend people and eventually at level 5 you can engage in conversations.' Participant: Does that mean if you are using the Met Twitter and you follow plumstead ... would that be legitimate?' Facilitator: Not quiet, as you are using a Met account you are being completely overt.	Participant: 'There are some things which I think creating a fise account for is perfectly acceptable for. Like when you have an online peadophile.'
How – Which aspects of the phenomena are being mentioned/omitted?	<i>Use of personal mobile device</i>	Participant: 'I think a lot of us are aware that we are not supposed to use our phones for this kind of research no matter how good our intentions are.'	Participant: 'I've tried using the work phone, its pointless.' Facilitator: And so you revert back to your own phones? Participant: 'Oh God yeah, we just revert back to wahtevers easy generally with all things.' Participant: It's easier just to use your own phone, your own minutes, i mean we all get free minutes now anyway, so it doesn't cost me anything to use my own phone.'	Participant: 'I've heard stories of [police personnel] doing snapshots of Facebook using their phones to look for a missing person.'
		Participant: 'The problem is that people are doing on their own phones, there is no record of what we're doing. People certainly aren't putting on any crime reports or Criminal Intelligence reports to say they are doing these checks.'	Participant: 'I find with AWARE you can't access stuff, it really restricts what you are able to do, so you have to go to your own device or a job phone for a lot of everyday things let alone anything else.'	Participant: 'Our social media is purely for good news stories and engagement with the public, I use my phone, my home computer because there's nothing coming back from it.'
	<i>Restricted Access to MPS IT</i>	Participant: '[Using social media of intelligence purposes] It happens all the time and is always done on their own phones because they're access to AWARE is restricted.'	Participant: 'The biggest thing I find is when AWARE blocks so much stuff on the Internet ... So a lot of the time we get videos sent to us that I can't view on AWARE, so I have to use my own phone to view the video via Instagram.'	-
	<i>Discipline</i>	-	Participant: 'I think everyone has been told don't do this and don't do that which has definitely made some [oficers] not want to do it [engage on social media].' [Group agrees] ... Participant: 'They don't have any kind of SOP either because I had the complaints department come and speak to us because someone had posted a picture of a samuri sword which didn't identify the person but they complained stating people would know it was him by the picture of the swords.'	Participant: 'People think [professional standards] are looking at everything, checking every story that you see. Every disciplinary to do with social media is because someone has posted something inappropriate.' Participant: 'It's people posting their own stuff, it's not you searching, it's not researching on other people it's people posting on their own stuff, people messaging each other with stuff that really shouldn't be going around, that's one thing bas as far as investigations or using your own phone to investigate, I've never see anyone disciplined for it.'

Thematic Coding	Themes	Focus Group 1	Focus Group 2	Focus Group 3
<p>How – Which aspects of the phenomena are being mentioned/omitted? (Continued)</p>	<p><i>Repeated Viewing</i></p>	<p>Facilitator: 'My feeling is that there is a grey area around the definition of 'repeated viewing' and what it means in practice.' Participant: 'I don't know, it's quiet confusing, it depends.'</p>	<p>Participant: 'Why can't I just have a look and see what all his tweets say. I had a case where we were directed to a graffiti artist on YouTube. So we have gone there, found him and taken screen shots to evidence the phrase linking him to the graffiti. But we don't know if we have crossed any intrusions. I did it and i didn't think i was, because it was all there, your just thinking its open source.' Facilitator: Well was there any 'repeated viewing?' Participant: I did it in the space of an hour and a half.</p>	<p>Facilitator: 'What does Social Media Surveillance look like?' Participant: 'Surveillance as opposed to a snapshot. It would be continual monitoring of all available social media.' Facilitator: 'Does it have to be repeated viewing or can it be a one-off viewing as well?' Participant: 'I believe it can, if you're not meant to be viewing it and you have, whether it's continuous or just a one off, you have still intruded in there.'</p>
		<p>–</p>	<p>–</p>	<p>Participant: 'When does a snapshot stop being a snapshot? When it's multiple viewings, is that multiple viewings of the same account, multiple viewings on the same day, same week, same year, is it multiple viewings for the same purpose or because you also looked at his friends?'</p>
	<p><i>Privacy</i></p>	<p>Facilitator: 'Is there any consideration around what the public might percieve as their privacy [on social media]?' Participant: 'I don't think they think about i. I don't think they think the police are going to look through their social media for any reason whatsoever.' Participant: 'If we have to circumvent privacy settings, then maybe that's a barrier, where authority may be required.' Facilitator: 'Then the onus of privacy is the responsibility of the people using the platform.' Participant: 'I think so.'</p>	<p>Participant: 'If someone is happy to put their world out on social media ... that's effectively what they are doing so is it our job to be responsible for those people and responsible for Facebook, Twitter and the like. They have privacy settings, we are fighting with both hands tied behind our backs because we are not confident to use [social media]. I think it comes back to clarification about what we can do as these are things that people are voluntarily giving us.'</p>	<p>Facilitator: 'What's your feeling about the last question on the privacy/security debate?' Participant: 'If it's a snapshot, a one off, for policing purpose, that's entirely different to then deciding to monitor one. Yes its open source but why are the police following? It becomes the definition of , 'what's a policing purpose?' Well we know this person's a criminal, so we will go and see if he trips up on there. So you dedicate someone to watching their social medai account or you are constantly doing snap shots on it to try and find something to get them for? Does it breach his right to privacy and family whether its on social media or not?' Participant: Just a new age way of digging! Participant: 'Fishing!' Participant: 'Yeah its fishing.'</p>
		<p>Participant: 'The same standards of privacy should be translated to social media [as they are in the real world].'</p>	<p>Facilitator: 'Do you feel once [information] is out on social media and the privacy settings allow it, then it is fair game [for the police]?' Participant: 'Yeah, yeah, I think its how it should be.'</p>	<p>Facilitator: 'How far should police officers go?' Participant: 'It should depend on the crime, it should be proportionate, a serious crime llike murder should [give you greater] access but if it's a petty theft then no you shouldn't be able to hound some poor person.' Participant: 'If someone puts something out on 'social' media then i suppose anybody should be able to look at it. If their posting stuff on Twitter, the same as a celebrity might Tweet and you follow them and look at them.'</p>
		<p>Participant: 'As I say if something is in the public domain then it is out there for everbody anyway. If you suddenly decided to target that person you would need justification.' Facilitator: 'But do we at that point?' Participant: 'It depends, if its in the public domain then are we being intrusive? No, because its in the public domain.'</p>	<p>–</p>	<p>Facilitator: 'What do you think the publics perception is of a state entity or investigative agency looking for their own purposes?' Participant: 'No, I don't think they have an awareness of it.' Participant: 'I suppose if their profile is on private, then they assume that its peer to peer rather than it can be accessed by higher up.'</p>

Thematic Coding	Themes	Focus Group 1	Focus Group 2	Focus Group 3
Why – Which reasons are provided or constructed?	Vulnerability	Participant: Say you're looking for a missing person. A search for their Facebook account, I would say is a basic enquiry. Looking at the person's social media and what they've said in the last 24/48 hours would be a basic enquiry.'	Participant: 'The one thing ... it does get used for by some officers on social media is when you've got high risk missing people, you'll search their name and see if you can get any information on them.' [Focus agrees because they are high risk] Participant: 'You can almost do anything, can't you? To protect the person!'	Participant: 'I've heard stories of [police personnel] doing snapshots of Facebook using their phones to look for a missing person.'
		Participant: 'It's immediate, if there's an immediate requirement and this person is vulnerable, a risk assessment has been done and we need to try and locate them ASAP. So the initial enquiries need to be done and I personally would think that an immediate look at their social media [would be ok].'	Facilitator: 'Do you feel that actually if it's a vulnerability issue [rather than an investigation] then the means justify the end in terms of looking at open source?' Participant: 'Yeah, you would often go to your Local Intelligence Team (LIT) team for this, but if it's a Sunday night or a night duty and no ones in, what else are you going to do. If you don't know there is 24/7 support you are going to look it up yourself.'	Participant: 'Its risk, its immediacy and proportionality. Is it worth checking [social media] to see where you have checked in in the last two weeks because you're a shoplifter? No. However, you are a regular missing person, you're a child and you constantly go missing at the weekend and I can see that you are at the same nightclub for the same five weekends.' Participant: '99% of the public would support that.'
	It's Open Source	Facilitator: 'Do you think we, as police officers should be able to just, if you have suspicion that a person may post something that gives him away or his position or who he is dealing with, the right to monitor?' Participant: 'Absolutely.' Facilitator: 'Just keep looking?' Participant: 'When I say absolutely, I mean allowing everyone to have access and knowing where the boundaries are.'	Participant: 'But we don't know if we have crossed any intrusions. I did it and I didn't think I was, because it was all there, your just thinking its open source.'	Participant: 'I think they understand (senior leaders) how powerful social media is and think we can exploit it. Even when you attend the Local Intelligence Teams you get inspectors not understanding the difference between running a snapshot for a missing person and running continual surveillance on their Facebook page.'
		Facilitator: 'What about investigations in contrast [to safeguarding]?' Participant: 'It should be down to the fact that it is in a public profile, that its an open public profile. Then I can't see any major issue because its out there anyway. I can't see any issue of going to somebody's Facebook account because we've done it before. It's an open profile. there is nothing stopping anybody looking at it.'	-	-
		Participant: 'The way I look at it if I were going to look up little johnny and what he is doing and I have been told he is on South Street, I would go to South Street, I wouldn't need RIPA because I am physically in full uniform going there, its not covert policing. In the same way, if that information is available at the click of a button and is available for everyone to view, I would treat it the same way. I would hope that we would be allowed to treat it the same way because it is open to everyone, so why should it be any different for officers.'	-	-
	Training	Participant: 'But see I view the problem of using police computers in terms of it obviously leaves a footprint. People need educating and training around that.'	Participant: 'You look at the training we got two years ago when we started using Twitter [for engagement]. The training now is completely different. The [MPS] has only learned from the mistakes we have made.'	Participant: 'I think [training] higher up as well to make it clear, we can turn around and say I am not doing it, but if you have a Duty Inspector who is desperate because they have a high risk missing person and you have Twitter, you access it!'
		Participant: 'Improve awareness of what to do if you need information for a warrant or need to follow the activity of someone they probably know is up to no good.'	Participant: 'There is no training on the Regulation of Investigatory Powers Act (RIPA) from the Department of Media and Communications (DMC). The training they provided details when you can post pictures and details of investigations but there is no training in terms of investigations and RIPA.'	Participant: 'I think with the training, Specialist Crime and Operations (SC&O) will get everything but the people who do the ground work is Territorial Policing (TP). I think if there is more training in relation to open source it should be rolled out fairly. A lot of the stuff we just don't get and the coppers need to do a job.'

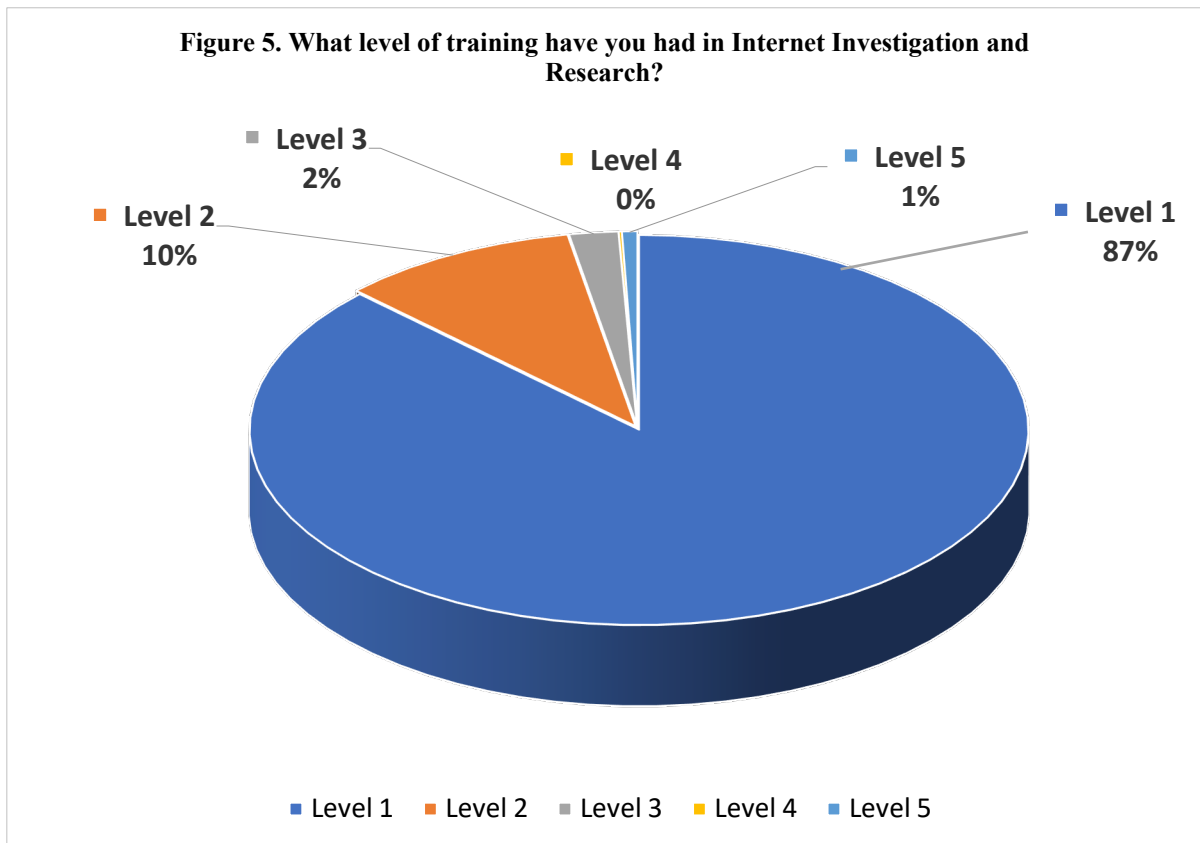
Thematic Coding	Themes	Focus Group 1	Focus Group 2	Focus Group 3
Why – Which reasons are provided or constructed? (Continued)	Senior Demands	<p>Facilitator: 'Do you think the organisation understands social media at the higher levels ... or do you think that people are just left to get on with it?'</p> <p>Participant: 'I think people are left to get on with it.'</p>	-	<p>Participant: 'I get it quiet a lot, a Duty Inspector asked me to hack into a person's Facebook.. I don't think they understand. Do they! That's them not understanding. Its been several times, can you get to this Facebook account or can you check this person?'</p>
		-	-	<p>Participant: 'I think they understand (senior leaders) how powerful social media is and think we can exploit it. Even when you attend the Local Intelligence Teams you get Inspectors not understanding the difference between running a snapshot for a missing person and running continual surveillance on their Facebook page.'</p>
	Policy/Code of Ethics/RIPA	<p>Facilitator: 'So we have said that these activities are taking place but are individuals intentionally going against current policy?'</p> <p>Participant: 'I don't think that [police personnel] know they are doing anything against the procedures, they think they are allowed to do it.'</p>	<p>Participant: 'I think a big problem would be if you came up with a MET Policy (SOP) for Twitter we would just be tweeting crime prevention advice [Group Agrees] and we'd have no followers.'</p> <p>Facilitator: 'Coming back from the engagement side what about guidance and policy around investigations and how to use social media for it?'</p> <p>Participant: 'Even less.'</p> <p>Participant: 'Yeah, there is nothing.'</p>	<p>Facilitator: 'What about the survey questions around MPS Policy and Code of Ethics, are these issues that officers are aware of or take into account?'</p> <p>Participant: 'I don't think there is enough knowledge.' [Another agreed]</p> <p>Participant: 'I don't think there is enough knowledge either.'</p>
		<p>Participant: 'RIPA demands that if we are intruding into someone's personal behaviour, authority is required.'</p>	<p>Facilitator: 'What about the Code of Ethics question, does anyone what the Codes are?'</p> <p>Participant: 'Yes, I wouldn't read that and think I have read the College of Policing Codes of Ethics.'</p>	-
		<p>Participant: 'The way I look at it if I were going to look up little johnny and what he is doing and I have been told he is on South Street, I would go to South Street, I wouldn't need RIPA because I am physically in full uniform going there, its not covert policing. In the same way, if that information is available at the click of a button and is available for everyone to view, i would treat it the same way. I would hope that we would be allowed to treat it the same way because it is open to everyone, so why should it be any different for officers.'</p>	<p>Participant: 'When I first read the question about RIPA, I thought I should know the answer to this.'</p>	-
		-	<p>Facilitator: 'In terms of social media and RIPA does anyone know how they interact?'</p> <p>Participant: 'There is no training on the Regulation of Investigatory Powers Act (RIPA) from the Department of Media and Communications (DMC). The training they provided details when you can post pictures and details of investigations but there is no training in terms of investigations and RIPA.'</p>	-

Appendix H - Survey Results

Question 1. To what level are you trained in Online Investigation (Open Source)?

Table 1.

Level of Training	Frequency	Percentage
Level 1 – Not specifically trained	685	87
Level 2 – Core Open Source Investigator/Researcher	78	10
Level 3 – Advanced Open Source Investigator/Researcher	17	2
Level 4 – Network Investigations	1	0
Level 5 – Undercover Officer Online/Covert Internet Investigator	4	1

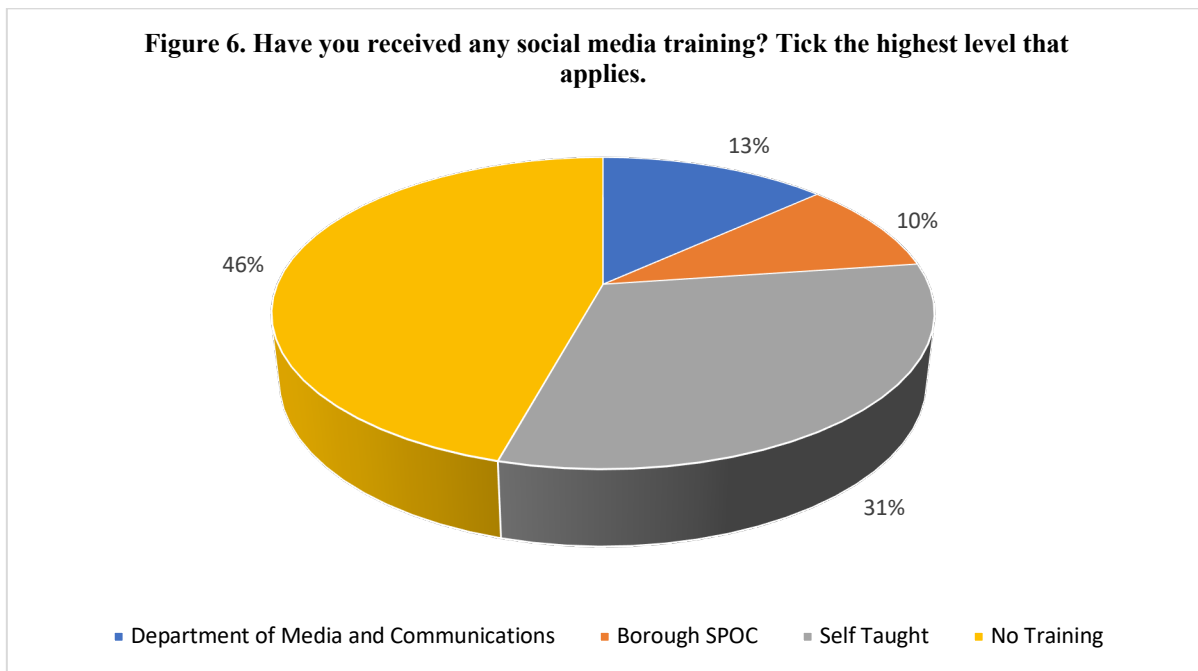


n=785, modal response – Level 1(685), Med=Level 1.

Question 2. Have you received any training in the use of social media? If yes, please tick all that apply.

Table 2.

Methods of Training Received	Frequency	Percentage
Department of Media and Communications (DMC)	104	13
Borough Single Point of Contact (SPOC)	75	10
Self-taught	247	31
No training	359	46

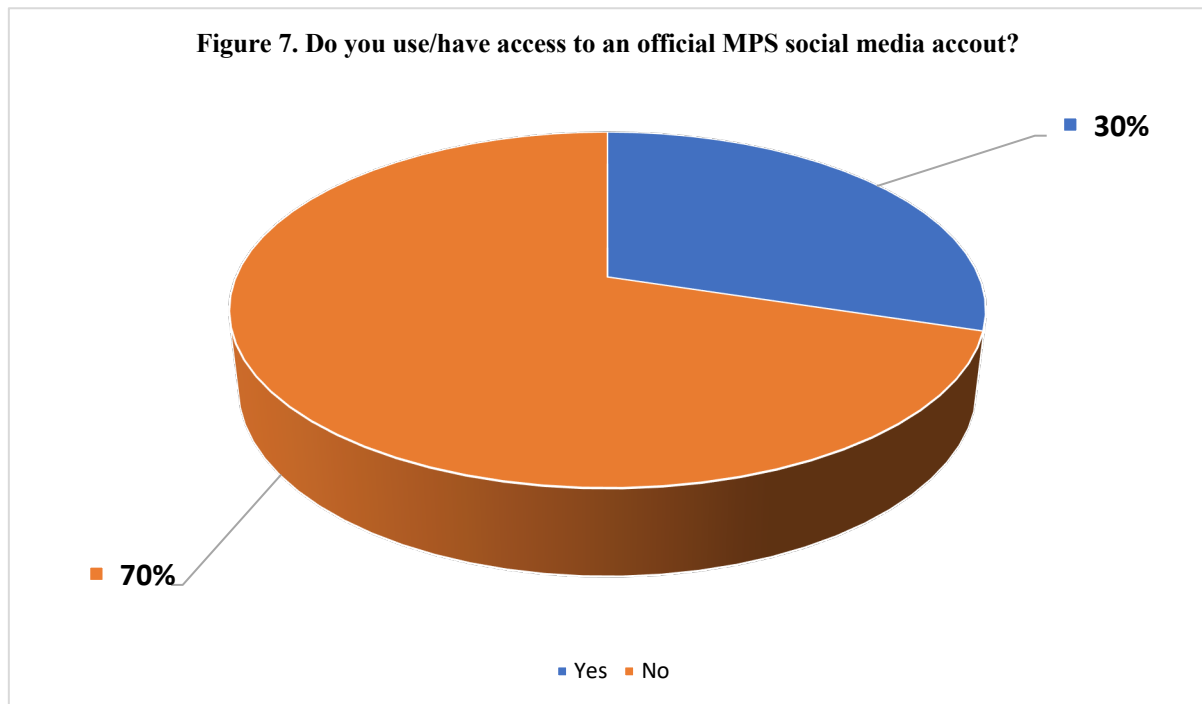


n=785, modal response – No Training (359).

Question 3. Do you use/have access to an official MPS social media account (such as @metpoliceuk etc.)?

Table 3.

Access	Frequency	Percentage
Yes	234	30
No	551	70

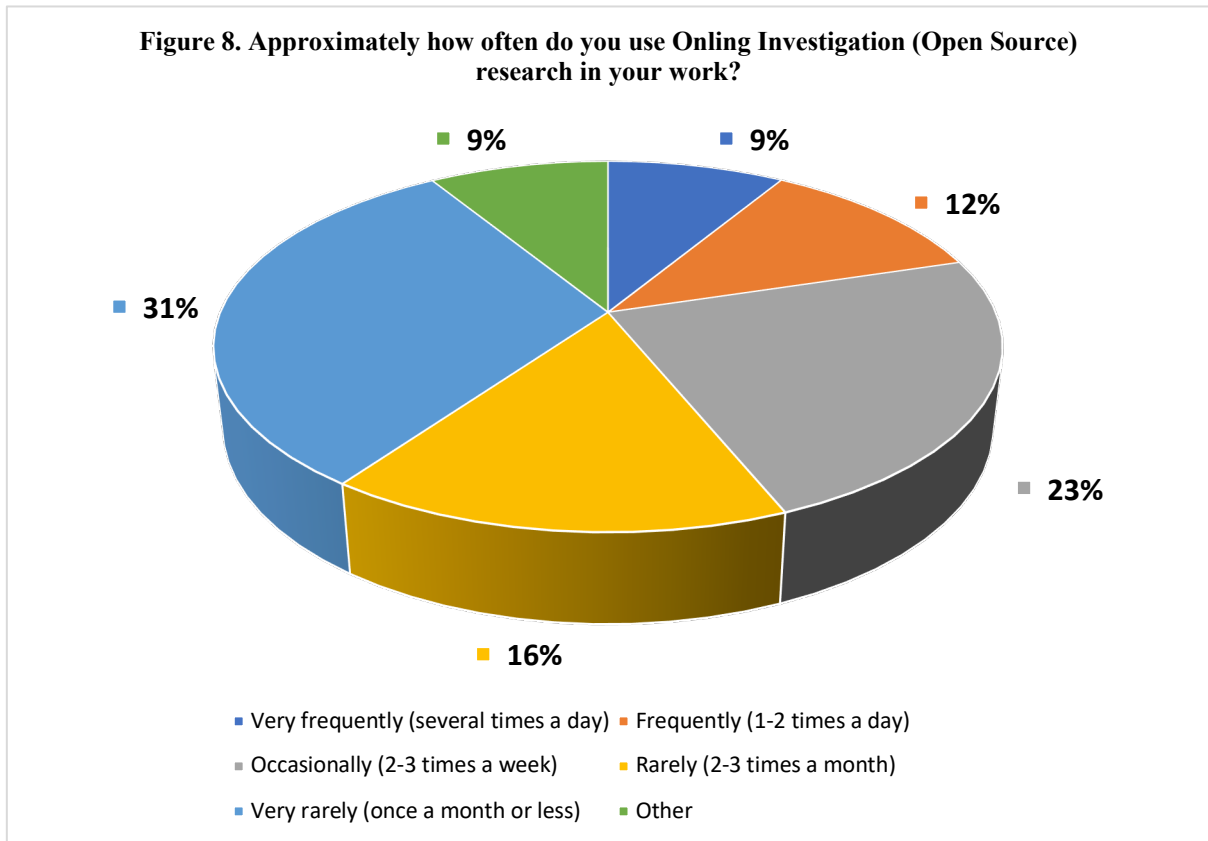


n=785, modal response – No (551).

Question 4. Approximately how often do you use Online Investigation (Open Source) research in your work?

Table 4.

Frequency of use	Frequency	Percentage
Very frequently (several times a day)	68	9
Frequently (1-2 times a day)	91	12
Occasionally (2-3 times a week)	185	23
Rarely (2-3 times a month)	126	16
Very rarely (once a month or less)	246	31
Other (Never)	69	9



n=785, modal response – Very Rarely (246).

Summary of Comments made by participants who selected ‘Other’ as an option:

Those who chose ‘other’ all wrote that they never use Online Investigation (Open Source) research

Figure 9. Qualitative Comments and Thematic Coding: Question 5. If you are happy to do so, please briefly describe how you generally use/have used Online Investigation (Open Source) research in your work?

Thematic Coding	Themes	Respondent Answer	Respondent Answer	Respondent Answer	Respondent Answer
What are the phenomena of concern being mentioned?		Q.5 If you are happy to do so, please briefly describe how you generally use/have used online investigation(Open Source) research in your work?			
Why – Which reasons are provided or constructed?	Investigation/Suspect	google to find if suspects/misps have been on used social media, intel on employers, business premises, google maps for potential addresses, to confirm location re phone intel (triangulation) gang terminology, street terminology etc	Gumtree, Ebay to ascertain sales of suspected stolen goods. Facebook to gain photo's of suspects and lifestyle information.	Searches to locate suspects / victims / witnesses / associates and for info on suspect that may be relevant to the allegation(s) made against them. Re investigations involving CSE (distribution of IIOC and inciting sexual activity) accessed the websites used by the suspects in order to ascertain what steps are required to register and use the website in order to get an idea of what digital footprint the suspect may have left behind.	Use in investigations to identify suspects, also used via open source trained colleagues for gang affiliation statements to assist in securing convictions at court, intelligence from youtube videos created by gang members and gang nominals twitter accounts in serious investigations.
		Investigation - Handling Stolen Goods (Pedal Cycles) Looking at sellers on Ebay and Gumtree etc	Looking into interactions between suspects and sexual offence complainants	General internet research, e.g scam building companies, legal questions, but don't use an open source computer.	Victim and suspect intelligence. Location of suspects and witnesses for investigations
		gang related crime, evidentially following assaults, etc. Bad character (youtube videos), to demonstrate association.	basic searches to look for suspect/witness on open source forums	Searching for owners of lost property, usually LinkedIn or facebook.	locating of suspects. researching victims.
		Googling suspects to see what comes up. Using Facebook and Twitter to look for suspects or confirm identities.	To obtain current photographs of subjects. To identify associates through subjects.	Seeking further information about named suspects or witnesses who don't appear on police indices. Misper investigations.	Used in investigations, to trace suspects, to establish if victims have contact with the suspect. For disclosure purposes.
		In the location of suspects	Entered suspect name on facebook to see photo	To assist investigations.	used the internet to locate find witnesses / suspects / phone numbers
		Social Media search request to help assist with locating wanted offenders	Searching phone numbers/names in Google/Facebook/Other social media	Used own device to assist searching for stolen mobile phones, tracking victim's friends down via Facebook for communication purposes, searching on Whatsapp and other social media.	I investigate CSE, and in order to identify subjects, their contacts, and to read messages/status updates they may have posted, Open Source research is used.
		Social Media search to locate evidence in an investigation, trained officer created profiles to assist with a sought video that showed similar fact offence to be used in court	Have requested Opensource checks		
		Used in investigations into CID main office crime where there is an online element (increasingly seems to be the case) and for high risk missing persons or manhunts.	Victims - to contact them after a robbery for example when they dont have a phone as it has just been stolen."	SOIS Officer using Open Source stand alone terminal to research info from comms data / Social Media	Location search and suspect/victim information checks and searches, general searches with regards to investigations. Facebook/Google...
		was used to track down suspects in jobs and to develop local neighbourhood intelligence around street names and associations	Trying to identify suspects and their locations on Facebook. Trying to access social media profiles to capture evidence of things posted to their accounts etc	follow prospective protest groups on twitter or facebook verified identities and/or associates of suspects checked addresses	use it to access open source profiles of people I am investigating, and also investigating topics about which I know little or nothing.
		Suspects in crime - to try and identify associates, suspects, etc	Two separate areas, counter terrorism work where the research would be conducted on a stand alone computer. The second is research on subjects and conflicts for War Crimes investigations.	Normal requests relate to suspects' social media accounts. Global searches for accounts and email accounts that may lead on to RIPA applications. Previously use open source requests to capture things displayed on the internet.	Facebook - to identify suspect whereabouts, friend groups. internet google searches for vague company details.
		To locate subjects who are either wanted or deportable	Trying to identify ISIS leaders or preachers or terrorist suspects or locations in the UK or the rest of the world.	Investigation into suspects and missing people	Wanted offender research and malicious communications investigations.
		This is used when conducting research especially when looking at historic offences.	Find out information about a suspect which will assist in affecting an arrest (e.g find a photo of them to enable identification). Assess lifestyle/pattern of behaviour for arrest strategy. To find personal details such a contact details for a suspect to enable further IP searches etc.	I'm not sure whether this question relates to a particular method or department, or is just asking how often I use open sources in my work. If it is the latter I use it regularly where pertinent (and proportionate) in investigating crime, usually related to someone in custody, due back on bail, who has missed bail etc. Unfortunately we only have one open source terminal which is used by the Local Intelligence Team so it's very rare I have access to something that can use evidentially.	To try and identify suspects using Facebook To check for undermining material relating to victims.
		This can be used to trace further victim's, witnesses and suspects or contacts within organisations that are no longer running.			
		research areas, subject profiles, business profiles	If I need to find a telephone number, an address, a route used or contact numbers for agencies. Or to find out about a suspect i.e. linked in	To view social network accounts of registered sex offenders to check contacts etc.	Investigation into an active OCN.
		1) Capture of evidence from a social media site, i.e. abusive messages.	Locating suspects. Suspect associates. General research on a suspect.	For Phased enquiries into EWMS subjects.	When a suspect is wanted by police to research potential locations/obtain contact details.
		used to help find suspect through social media	To find owners of lost property, to check locations of venues and verify information given by people, to find the names of wards/SNT teams	Looking at addresses on google maps to plan deployments. Finding people on social media - suspects/misps/restoring lost property.	it helps trace outstanding suspects
		the borough IOM Unit's Enforcement Team would aim to use OS to locate and arrest members of the cohort unlawfully at large.	WhatsApp - by adding a SUSP's number to phone via number provided, we were able to obtain an image of them, as they had their photo as their profile photo. They cannot tell that we have added them just by our saving their phone number to our mobile phone.	i am based in the volume crime unit which deals with various offences such as harassment, lending letters, mal comms, obviously the majority of this happens on social media and we regularly have to carry out research on suspects not just to prove the offence but for location and apprehension. i have to scout around for somebody who is trained and free to assist.	Identifying suspects from social media accounts, tracking suspect's historical movements (eg were they in the UK at the time of the offence), making familia/friendship links, tracing ongoing feuds/arguments/relationship breakdowns, bad character for suspect and victim
		The Engagement Team (my side) would aim to exploit OS to identify associates, indications of offending (or abstention from offending), risk management and lifestyle in support of operations by central squads. We would use it to obtain clothing descriptions, linked VRMs, addresses and details of girlfriends, locations frequented, the state of family relationships. To confirm or deny stories given to partner agencies. This kind of work has an almost fractal nature, the amount of intelligence you can obtain is only limited by the amount of time you can spare. It's an incredibly useful tool and the proliferation of Social Media Apps means the intelligence available	Otherwise was not aware we were able to access Facebook / twitter / other for intel purposes, although I have done this o/s the MPS in my day job (I am MSC).		
		Examining the social media of victims and suspects in sexual assault cases	To identify gang members in homicide enquiries and other suspects.	mainly used to look at social media profiles of wanted offenders /or subject of long term investigations	this is a great tool to identify suspects, trace were abouts, and find missing persons
			Type in suspect names.	To locate suspects	To search for wanted people
In CID we regularly research	intel checks, open source information to	To identify suspects or person of interest or associates of	In order to identify suspects. If a name is		
Often used to link suspects together in linked	In the gangs unit we frequently have cause to	Research for suspects names using Facebook etc.	I have used twitter to disprove an account		
as a schools officer kids use social media to committ	Researching persons of interest in	Locate and identify outstanding suspects	have contacted Gumtree & eBay for		
I have requested research into social media	when searching for a person where	We have used in the past Facebook to assist with	domestic		
basic facebook search looking for suspects	Investigating bus companies and the	Using google maps for CCTV enquiries or for locating the	Identifying and tracing suspects.		
When you have a suspect or person you cant trace	Investigation of cases re online hate crime	TO LOCATE VICTIMS OF CRIME - I.E. PICKPOCKET VICTIMS	Mainly within my role as CSE Spoc on borough		
High Harm Manhunts, High risk Misps, Covert	Tracking offenders who are wanted. I would	will occasionally look on the internet (i.e. Google search)			
my open source is to ID suspects & background checks on witness/victims	Use internet maps. Investigate company links for suspects. Research for suspect identification, missing person enquiries.	Wanted offender enquiries and for domestic abuse related offences such as harassment, malicious comms and sharing private sexual images.	Obtaining email address's or telephone numbers of victims.		
Use of daris, crimint and cris to identify suspects and victims currently on my ward	am part of the East Area Proactive Unit and I used open source to assist in conducting man hunts. This helps a lot.	Researching suspects through social media, background research on companies and employees.	Primarily in criminal investigations/Intelligence around EWMS suspects.		
To find contact details for premises, to determine likely routes travelled by suspects, to get a clearer understanding of a venue/location detailed in a crime report, to get a background on a suspect.	Looking for addresses via googlimaps searching for business addresses searching for social media profiles for outstanding suspects	i use this and would use it more if access was better to looking for offenders and any indication of their offending which they may post of social media. Also opens source such as the voters register, LinkedIn etc.	Hunting suspects, identifying suspects		
Researching witnesses, suspects and persons of interest in my investigations.	In child protection cases, mostly historical, identifying where suspects are and locating first complainant.	To help identify and link offenders	Facebook for suspect photos or associates etc		

Thematic Coding	Themes	Respondent Answer	Respondent Answer	Respondent Answer	Respondent Answer
What are the phenomena of concern being mentioned?		Q.5 If you are happy to do so, please briefly describe how you generally use/have used online investigation(Open Source) research in your work?			
Why – which reasons are provided or constructed?	vulnerable	I have asked for open source checks in relation to missing persons. Whilst working on the misper unit - open source research on for example Facebook was a great tool for monitoring some of the mispers who were out of 'contact' but would post on social media at least we could establish that there were alive and seemingly well .	Investigation into suspects and missing people It was used to obtain an idea of proof of life etc for missing people, it was not used as a replacement for a proper debrief but it added to the risk assessment to see if there were any sudden changes in behaviour. The public image was also useful for up-to-date images of the missing person where there were not always current images from their family.	In trying to identify sex offender on line identities or to establish profile for missing persons. For fast time research on intel about possible raves and bike/leisure events on Borough as part of the Hot Desk Sgt role within Borough GPC Also trying to research Mispers and to identify addresses that are new developments not shown on current MPS Mapping software or known to the CAD system.	Facebook for photographs of MISPERs To assist in identifying and locating offenders/mispers and to assist in investigating evidence of offences on line
		Missing people - to try and identify friends names/addresses for them.	For information on Mispers: identification of critically injured persons in RTCS	Usually for Facebook enquiries for missing people or for investigating crime	During missing person investigations or where social media public order related offences are reported.
		Searching and risk assessment on MISPERs, identification of social media accounts, ISP.	Missing persons investigations - high risk	social media like try and check Misper social media accounts , or fb	Misper engs
		Mostly used to research high risk missing persons, to ascertain social media use, friends etc and if there is anything useful on their profiles.	Use of sites search facilities within Facebook, Twitter, Pipl, Google, Bing to identify and research internet presence for suspects, victims and MISPER	To track movements from High Risk missing people	I work in the Misper/CSE dept. It is useful to look at locations/places frequented. Peer associations and photographs can help with confirming identity.
		I am involved in missing persons and CSE related to children. The social media provides a better insight into investigating these types of offences better than any other METR system.	Misper Enquiries. Information around offences. (CPS)	Identifying partially known suspects or locating missing persons	Missing persons and generally cyber crime to do with young persons or young people posting suicidal posts
		I work in a Borough Missing Person Unit and as about 70% of our work is looking at peoples face book accounts we have all set up individual face book accounts in our names with our Met Police Email addresses. That is the only social media platform that we can access. We are waiting for a smart phone to be allocated to our unit to enable us to access WhatsApp. Social media is a significant investigative tool. We will request Open Source checks but often we are asked what social media platform checks we have done prior to	Open source investigations can be very useful when dealing with missing persons, where time is of the essence. Nearly everyone has some form of electronic footprint these days and to be able to use these platforms is extremely useful.	Normally around locating high risk mispers or high risk suspects. I work on response team and this is when no one is available with an approved Facebook account. This is when the research is time critical. I know I should not but for the sake of expediency I have created a Facebook account solely for this purpose.	Using google maps for CCTV enquiries or for locating the scene of an incident. Using an informant's snapchat to track movements of Mispers if they have their location active.
		Investigating high risk missing people through their use of social media	as duty officer require open source intelligence for variety of situations forming missing persons through to public disorder	Locating/researching missing persons, regularly use Facebook, twitter, Instagram.	Researching social media to find "friends" of MISPERs. Using Social Media to message MISPERs, regular TWITTER on behalf of Borough and SNT
		Social media: events happening in my ward (UME/Raves), names/nicknames of people encountered in investigations.	When researching I routinely use open source routes to corroborate information, evaluate weight and assess options to progress.		Its useful to look at gang members online profiles, their associates and activities.
		I just want to view youtube videos and the odd facebook page for researching large music events.	2) Research locations and events e.g. tracing the landscape in the background of a photograph sent by a missing person."	Normally for operation planning, using Google for maps, images of venues, etc.	Open Facebook profiles and Instagram accounts.
		to find people's full names and addresses, finding them on social media and completing searches on Met Police Systems to cross reference and see if I can find the relevant information	To find the online footprint of persons of interest, to identify lines of inquiry, contact details, etc	Establishing post codes for various addresses, for crime reports and other purposes. Location/mapping to establish directions for MOP. Use of Google maps and Google earth for briefings etc. Use of twitter for contacting the	Linked in for vetting purposes
Front Office enquiries - Property, Suspects	Personal research on addresses/post codes via mobile internet	To validate phone numbers, addresses, locations, companies house. Don't use social media to review persons of interest.	mainly used for address searches		
Manhunts Evidence Gathering Witness Appeals Appeals in general Intelligence Gathering. Generally, if something might be online, I use the internet to find it!	We would use it more but not open sourced trained. Gang member Facebook/twitter/instagram accounts can provide vital evidence of assaults, drugs weapons carried etc.	Searching for locations, buildings and unfamiliar addresses. Can sometimes be used to help in planning patrols. I have used the internet in the past to establish the veracity of claims made by somebody I was dealing with. Very useful indeed. Sometimes use internet to look up news or current affairs which affects us in the workplace.	CT Protect Borough Support Officer: Use open source searches on internet to find back ground details on events and venues, no requirement for any covert searches.		
Operational Planner needing to research festivals around acts playing	researching gang members	using facebook and/or Twitter to get information about events	Have previously used social media sites to try and obtain photographs of suspects and/or Mispers.		
I have used both MPS internet facilities and my own personal devices to conduct basic open source research, such as reading Facebook, Twitter and public websites - in my case usually ticket websites such as Shobos for information regarding music events.	frequently use the internet to investigate addresses and telephone numbers. Often have a requirement to conduct research on offenders social media accounts however as I am not personally trained this work has to be farmed out to other departments.	research in to gang members and their associates. fast time intelligence in to gangs re youtube facebook and others social media account.	Googled various questionable 'business's' to find out legitimacy for an investigation. I have used to find information on an address for a warrant execution.		
Investigate improper use of social media by students at school	Borough Event Planning, for large scale events to identify Facebook and Instagram account user identities/activity	Assessing Community impact after events. Corroborating intelligence received to manage risks. Tracing Missing persons.	Looking for potential companies etc regarding suspects/victim details		
Business phone numbers and locations etc. Identifying potential social media accounts to provide to open source to complete research.	input of telephone numbers into social media	Search suspect phone numbers, emails, IP addresses on Google before completing OPTICA applications.	Fed Rep - Research for case and work related items		
Very rare I use in current role. If it is it is to find out information on a venue or guests that the BOCU Cmdr will be meeting.	Intelligence around OP VENICE / motorcycle theft	Looking at Facebook accounts/pages relating to illegal raves	Obtain personal details from social media usernames.		
Google, rand fraudulent phone numbers through IIP, no hits, Google was able to identify the number as a scam	Use search engines for phone numbers related to vice to find any websites related or for house address/google instant view to see what an address looks like. To get contact details of businesses/individuals. Sometimes to access legislation websites to check points to prove.	Voters checks, Facebook vis Misper unit, GB Accelerator via other officers.	When investigating two crimes where suspects have decamped and information on the suspects was given Met Intel contacted and the relevant forms completed for them to undertake the request		
Confirming locations, establishing routes to and from locations, obtaining contact details, gathering information, locating suspects, identifying subjects, researching legislation, researching best practice, identifying new resources, language translation, travel arrangements, interpreting data (such as converting ANPR co-ordinates into Google Maps).	I used to use it to locate stolen goods sellers in our area e.g. by looking for easily identifiable LOS property amount items for sale on line. Or a local seller selling multiple pedal cycles. We were trained very briefly in Ebay stuff a course called EOP's but the MPS stopped subscribing so we now have no access.	Use internet to check location for research (crime investigation / officers safety risk assessment / pre-planned operation etc) Use internet to check on victim / witness (risk via media profile) use twitter to search for evidence - noped enable offence	if deployed as an Intelligence Gatherer, before or during the event, usually a public demonstration, I have used my own personal twitter account to search relevant hash tags to get an understanding of the mood of the demonstrators any any potential target locations. If I have ever found a possible target venue, I have alerted the relevant intel pod at GT.		
Open source on social media provides valuable intelligence on subjects under investigation so at every opportunity social media is checked for latest photos, personal information on whereabouts both past and current. This can be used obtain information which can then allow police to apply for further apps.	Search engines such as Google, Piple, Bing. Search for social media profiles primarily on Facebook but also on others using name, phone number or email address in order to identify relevant accounts to further an investigation. For example, subsequent CIU/RIPA application	I use it to identify issues that may have occurred on my ward and to also obtain details and what the subjects are known for those I encounter causing current issues	Gain access to media sources/social media sources pertinent to job role. ie university liaison officer - universities + university societies use those sources to engage with their audience.		
Used to research suspect's for various levels of criminal investigation. Used to identify and locate suspects and their criminal associates, platforms such as Instagram, Facebook and twitter.	I recommend it in finding wanted persons and it can also be useful to gain information as part of an investigation.	searches can identify addresses & locations; reveal proximity and also provide pictures relevant to the investigation which I have exhibited. searches can also identify new witnesses/suspects to obtain statements from or interview. various documents have been printed and I have exhibited them for Court.	I am a Licensing Officer and often need to risk assess applications for late night events or Crimints relating to potential illegal events / raves. A private birthday party for friends / family may be shown to be a commercial concerns when the site advertising ticket sales is located.		
SUS research, phone numbers addressed etc.	Find addresses and postcodes, telephone numbers	Research into proposed events on licensed premises.	Immigration work, checking location of places and details given		
I was made aware of it by KF Gangs when ding some research on a Borough nominal	I regularly search the internet and social media for Intels and Info purposes to help and assist with events planning. Although we have a IIT team, they are often busy with other requests and mainly deals with crimes rather than public order.	Use of government website for up to date info in relation to mot status of vehicles and potential defects also Google maps and Google translate to enable communication with non english speakers.	Also used to build subject profiles to demonstrate the suspects quality of life. (excessive cash spending, purchasing high end cars and often openly using drugs on social media		
Usually through Google, checking locations or building frontages via google maps for warrants to confirm crime legislation, again via google whilst out on patrol.	Used VRM 'we buy car sites' as interim measure when PNC was not available. Google street view to assist warrant planning.	Looking for more information on suspects for offences - location, images of them, etc.	often use google to assist in research of certain topics and laws not commonly come across e.g. dogs act offences in order to obtain a better understanding and examples to assist my learning		
my role requires me to book venues / events and use web based sites to submit reports.	Before during and after public order events	Use twitter for engagement and monitoring when critical incidents	Companies house checks, phone number research on those used by suspects/victims, google maps and satellite view.		
I work in CSE which requires OS work on every suspect before any CIU actions can get the go ahead. OS is very useful to my area of work and usually reveals some useful information.	Primarily I carry out research on emerging trends ,the wording of, the location/s of and the and cultural practices across the world relating to the offences. I investigate the operations I plan, the community relationships I build	Googling addresses, street view to see if vehicles are in locations, how premises are laid out. Zoopla searches for floor plans prior to premissis searches. Identifying communications service providers prior to RIPA requests.	If I am putting someone's details through IIP I usually also put them through Google. This happens most days.		
To look at stakeholders, Read business proposals Anything and everything possible to do with SNT	Working in the Local Professional Standards Unit to look up businesses being run by officers who have not declared a business interest.	To check locations provided in reports	Use publicly available information such as DfT data for MOT / Operators and Companies House for director information.		

Why – which reasons are provided or constructed?

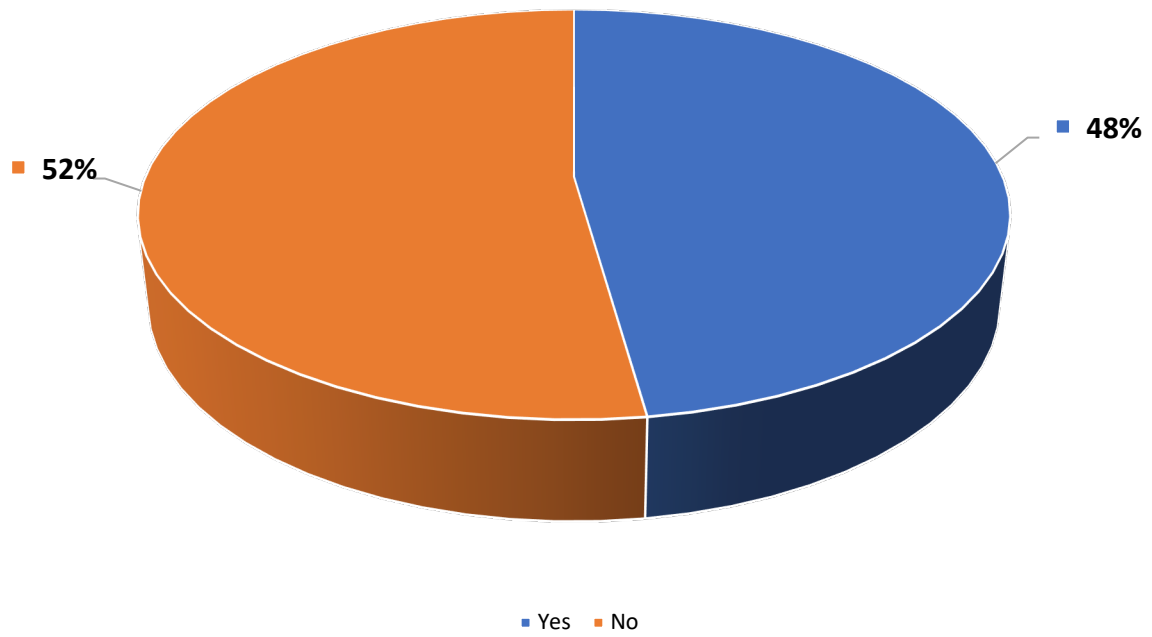
Intelligence

Question 6. Are you aware that the Open Source Unit (OSU) at Cobalt Square is able to conduct Online Investigation (Open Source) research on your behalf?

Table 5.

Awareness of OSU	Frequency	Percentage
Yes	375	48
No	410	52

Figure 10. Are you aware that the Open Source Unit at Cobalt Square is able to conduct Online Investigations (Open Source) research on your behalf?

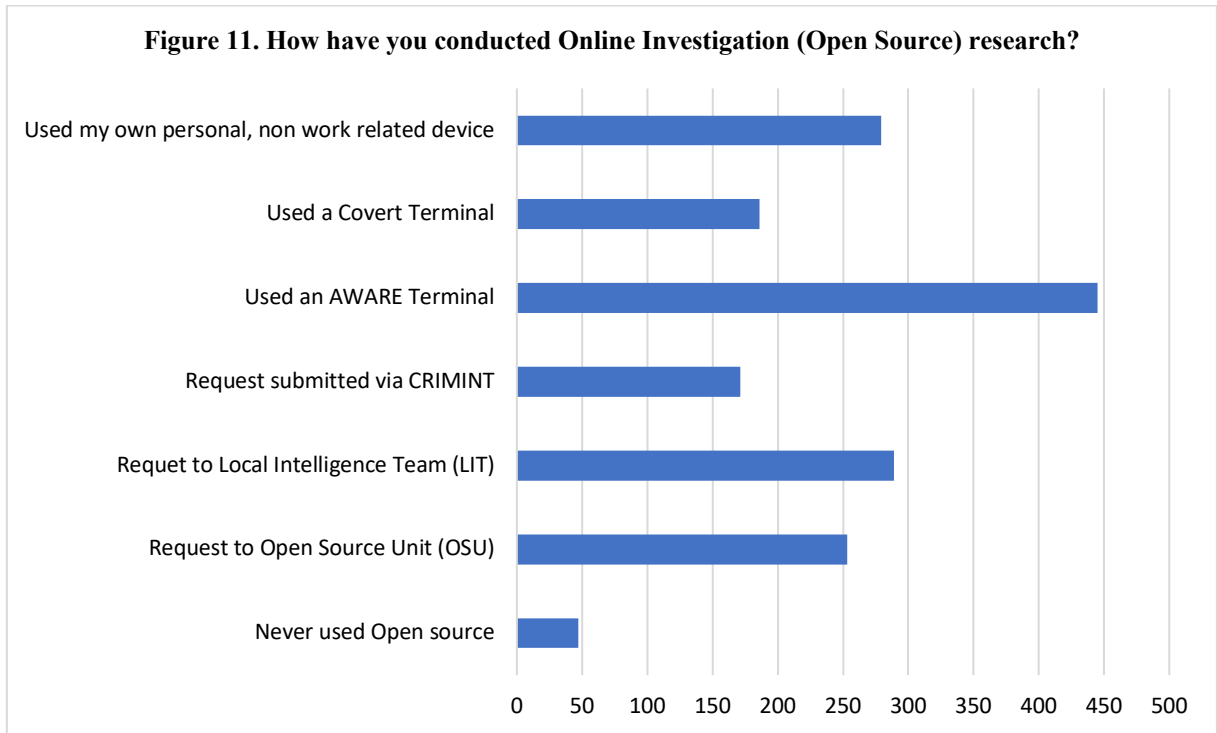


n=785.

Question 7. How have you conducted Online Investigation (Open Source) research?
Please tick all that apply.

Table 6.

How was Research Conducted?	Frequency
Used my own personal, non-work-related device	279
Used a Covert Terminal	186
Used an AWARE Terminal	445
Request submitted via CRIMINT	171
Request to Local Intelligence Team (LIT)	289
Request to Open Source Unit (OSU)	253
Other (Never used open source)	47

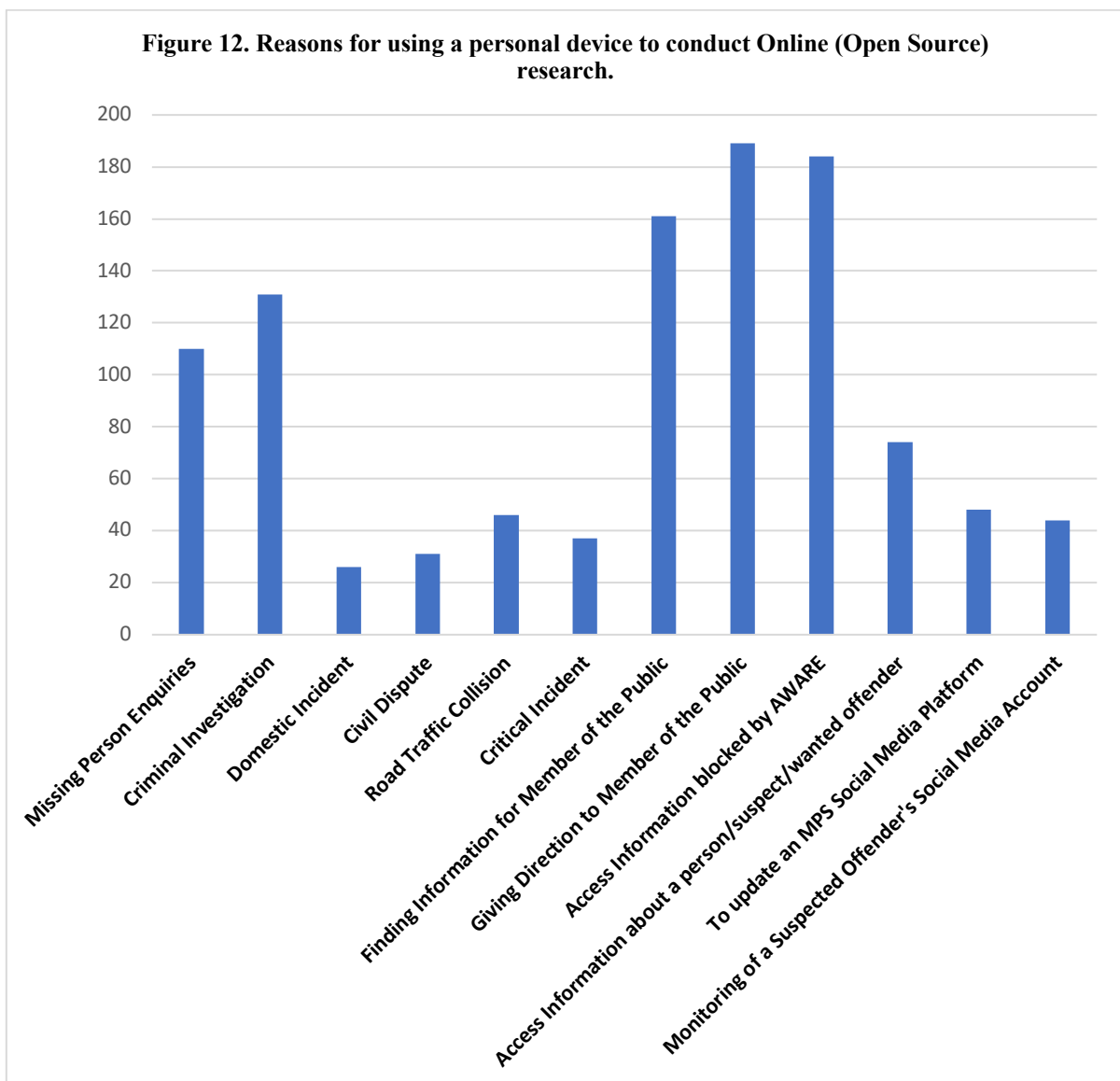


n=785 Respondents.

Question 7.1. (If personal device selected as a response to Q.7)
 For what reason(s) did you use the personal device to conduct Online Investigation (Open Source) research? Please tick all that apply.

Table 7.

Reason for Using Personal Device	Frequency
Missing person enquiries	110
Criminal investigation	131
Domestic Incident	26
Civil Dispute	31
Road Traffic Collision	46
Critical Incident	37
Finding information for member of the public	161
Giving directions to members of the public	189
Accessing information about a person/suspect/wanted offender	74
Access Information blocked by AWARE	184
To update an MPS social media platform	48
Monitoring of a suspected offender's social media account	44



n=279 Respondents.

Figure 13. Qualitative Comments and Thematic Coding: Question 7.1

If Possible, please provide further details of the incident/occasion to help us understand why you used your own device.

Thematic Coding	Themes	Respondent Answer	Respondent Answer	
What are the phenomena of concern being mentioned?		Q.7.1. If possible, please provide further details of the incident/occasion to help us understand why you used your own device.		
Why – Which reasons are provided or constructed?	Directions	Whilst on foot patrol, numerous members of public asking for directions, asking what buses they need, checking bus times, store opening times,	Maps won't allow desk tops or tablets into you tube or many social media but I can use a huge amount of law	
		Directions and advice to elderly passenger on bus. Advice about Help the Aged and useful contact numbers.	with regards to directions / information for the public, we are expected to know EVERYTHING and get complaints of being unhelpful if we don't and suggest they use their own smart phone they are holding in their hands as they ask their question."	
		Usually to identify locations on a map etc.	Map application	
		Out on the street you may have to use google maps to help with giving directions	Google maps for when the MDT won't log on, particularly because of the accurate house numbers.	
		Directions and to promote work.	Address/post code search	
		Directions given to MOP in central London, best way to show them on a map where they are and where they need to go. Also checking postcodes and directions to them when attending a call.	Directions and advice during public order. To educate myself on the stance and view points of demonstrators prior to a PLT deployment to enable me to communicate with a better understanding.	
		directions given on the street and personal device is only available	On Aid in an area I don't know well. Wanted to help member of the public by using maps on my phone to give directions.	
		Anyone asking for directions		
		Wanted person who had a semi open facebook profile. Could see that they were out of the country. Also a victim of crime found their stolen bike on gumtree. Looked at the details of the advert.	Checking websites in relation to fraud, where Aware otherwise would block searches.	
		fast time enquiries on street or OMPD.	They need to show me the snapchat messages etc so I can see their part and what the other party has done	
		Whilst making enquiries with a witness to identify a suspect and was told he had a Facebook profile. I logged onto Facebook using my own account and they identified his profile for me so I print screened his profile page and sent it to myself before logging out again.	Social media incidents and students cannot access the accounts due to school blocking / no data	
		Wanted to search for detail of a suspect and related witnesses on a facebook group. Did not want to leave a met police footprint on the facebook search, also do not think we are supposed to use facebook on aware computers?	To look up linkedin to look at a photo to confirm a victim was the person I was looking for and where they worked.	
		Used own device to assist searching for stolen mobile phones, tracking victim's friends down via Facebook for communication purposes, searching on Whatsapp and other social media for photos of Mispers/wanted people if not on custody imaging.	Used own device to assist searching for stolen mobile phones, tracking victim's friends down via Facebook for communication purposes, searching on Whatsapp and other social media for photos of Mispers/wanted people if not on custody imaging.	
		Trawling social media quickly reacting to information from a victim to determine if the information was accurate and would lead to a potential suspect being identified. Once confirmed that the information was accurate I then submitted an official request to have the social media account evidentially captured.	Track a Romanian burglar who created a number of profiles. Male had not been arrested before and we could not locate him. Used Facebook to try and discover friend groups that he was associating with and locations of picture he was uploading.	
		Open source research of information in the public domain relating to historical information to assist in linking subjects, locations	searching for organised crime suspects and associates	
		Looking for any youtube videos which may have been posted of the collision to use as evidence. Used my own device as Job computers do not allow access to youtube	Lots of incidents when trying to access websites and social media profiles to obtain evidence.	
		Investigation relating to betting Office. unable to access website because blocked on aware.	Looking at pictures on Facebook is quicker on my phone. A large rave had taken place and pictures had been uploaded ot Facebook. I was looking at the pictures to identify the organiser.	
		I have used my personal mobile and tablet to see facebook profiles and gain info from the press. It is the quickest way of seeing the information that is in the public domain.	I have used my personal device to look at profiles of suspected brothel ladies in relation to phone numbers being advertised	
		Another case involved harassment and this involved requesting LIT team to interrogate the facebook account for images of the suspect"	I had a hate crime involving a post on facebook and the suspect had images of the area around his house, this was identified from google maps and then voters.	
		I fully understand why many seemingly harmless internet sites are blocked on MOS Aware terminals - internet security is of course very important but it is a nuisance! I am involved in offender management (low level stuff on borough) trying to monitor IOM nominal and also trace outstanding wanted persons	As when trying to locate possible named SUS would look at FB for a possible sus pic	
		Complaints investigation for details of potential witnesses and to view maps etc when	Social media to invalidate a defence	
		vulnerability	Used map function no mobile to direct a MOPs. Used Facebook to explore family ties following the creation of a Merlin	Sometimes need photos of misper urgently.
			Understand lifestyle of person in minutes as opposed to hours - Crime and misper.	No other suitable access to internet available on the street. Obtain local partner agencies contact details to assist with helping a vulnerable person.
			Facebook searches for missing persons because I don't have an MPS account."	Mobile unit on missing person investigation. No access to portable MET issued device.
			It has been used to for high risk misper enquiries. It is used to search for suspects.	High risk issing person - needed to identify a landline telephone number and company name.
			Female critically injured in RTC had very rare surname. Used Facebook to locate potential	Misper's location.
			Fast time enquiries into sex offenders and High Risk missing persons.	

Thematic Coding	Themes	Respondent Answer	Respondent Answer
What are the phenomena of concern being mentioned?		Q.7.1. If possible, please provide further details of the incident/occasion to help us understand why you used your own device.	
Why – Which Reasons are Provided or Constructed?	IT System & Restrictions	Where there is no aware terminal available or AWARE blocks the site. I would not log into my own social media account to search, but only use publicly accessible sites.	I have used the internet to look at venues that feature in investigations."
		Websites frequently blocked on Aware, most recent example being a YouTube video linked to a gang-related murder that could not be viewed on Aware. Everyone on the MIT team had to view the video on their personal phone. Google Maps is unusable on Aware via Firefox.	To access certain websites for night club venues which are blocked by aware. Access required for research purposes into events and DJ's. Our current job issues device(Blackberry) does not provide this to a satisfactory standard. "
		When I am out of the office until very recently I did not have an MPS issued mobile device that I could use to access the internet.	Own device has been used when websites are blocked by Web Marshall or out of MPS building.
		Research frequently conducted using Google Street View which has to be conducted via Google Maps app on personal devices. Internet access on Aware is sometimes so slow it's just easier to use you own device.	Until recently our computers were only running XP and were so slow that I brought in my own computer so that I could be far more efficient at work. Social media is used by everybody today and I can not believe that the MPS are so slow to act to bring us to speed.
		Website blocked unknown reason eg. of University while looking for contact details, Misper description from Facebook, Aware terminal crashed/frozen or general ease of access, locate info from TFL e.g. precise bus stop details for Cris report [letter, name, direction, etc]	I recently tried to access Ladbrokes website to obtain details of locations of their betting shops in a particular area, but the web marshal blocked it because of 'gambling'. It is lamentable that in this day and age a Scotland yard detective is prevented from accessing websites to try and obtain important information to assist an investigation, just in case he might 'place bets' or 'view pornography'????? Where is the trust element, treating staff like adults etc
		Unable to use work desktop as block, out and about assisting members of public.	To find open source items when no access to a terminal normally fast time. Also to look at legitimate business sites that have information provided by premises used by suspects. social media sites have only been search via a medium of google to prevent me leaving a digital foot print behind.
		To google information as the work computers take too long	no access to information using work terminals. Eg checking social media for missing people and accessing blocked websites.
		MPS systems are not up to scratch or capable of conducting most but the most basic research. I have attempted to get LIT team to do research but the mailbox was not monitored real-time and by the time I got a response the opportunities would have been lost."	To establish what I was looking at. A victim of Rape stated that she met the suspect on a site called Whisper, so I researched Whisper to see what it was about.
		I occasionally look at You Tube videos that are blocked by AWARE (You Tube ONLY - I am aware of the security risks to myself by clicking on other - less reputable - websites). "	MPS terminals make me want to die
		Lack of provision of suitable hardware by the police. When on the street and information is required there and then it is easier to use your personal device rather than wait on the radio for someone to check it. If every officer had a job issued phone that was fit for purpose then this would be eradicated.	Mainly because sites were blocked on Aware when investigating brothel closures.
		It happens multiple times as the aware terminals are quite restricted, the stand alone terminals are few and far between (or hidden in a proactive teams office), it is usually the quickest and easiest way to carryout the task at hand.	I would only use my own device if there is an issue with aware and it wont allow me to access the information i need.
		This was blocked by aware as it decreed it business use.	In general terms, MPS technology is so poor, slow and unusable, that to get the job done you have to use other means.
		Due to the fact the MPS systems are slow and not user friendly or at that time not readily available for use.	could not access linked in as confidential work station
		Cant access social media account via aware, no other easy way to do so	AWARE not available or is slow
	Being blocked by job firewall	Better access to certain social media platforms (snapchat username searches/Instagram)	
	Youtube and videos are blocked on aware terminals. However, colleagues and I have been part of videos filmed by DMC or have crime prevention videos which we want to promote on met social media but can't view unless view on our own devices. Once the video has been viewed, I then share it on social media using an aware terminal as I now know the content is suitable.	Because the Aware system blocks us from so many websites its easier to use my phone most of the time. Or I use my phone when im out on patrol as its quicker than the brand new tablets we have been given.	
	As an Liaison Officer I needed some info from websites that were blocked by Aware. I also use both the Twitter and the NCDV apps on my personal mobile.	Checking facebook and twitter accounts of a suspect. No access to MPS log ins to be able to check details - Was required to log in to proceed further	
	Its Open Source / Covert	Aware is slow and security settings often preclude this - some data is large and the Met systems cant always handle the download bandwidth.	Those times when I am away from the office and want to check info about an event.
		WhatsApp - by adding a SUSP's number to phone via number provided, we were able to obtain an image of them, as they had their photo as their profile photo. They cannot tell that we have added them just by our saving their phone number to our mobile phone.	Social media sites blocked on aware terminals.
		Vehicle blocking road. Keeper details checked using IIP to try and contact the keeper to move vehicle. Keeper was a company and internet used to look at web page to obtain contact details. The driver was then contacted and moved vehicle.	On aid to ascertain football results at other local clubs in anticipation of increased tensions of supporters when leaving the grounds after a match as a neighbouring club."
		Details provided to another member of public regarding Citizens Advice Bureau.	Social media sites blocked by MPS. Covert terminals not available
		To identify location of an organised event where no risk to self.	Short staffing means longer wait times to get the information needed quickly. Tablets have now been issued so this should prevent the need to use personal devices
		The MPS aware terminals do not load twitter correctly so it is easier to do it from my own phone.	Especially looking at events and groups on Facebook which normally on MPS aware terminal wont allow you to access certain pages without logging onto Facebook. If I require to screen shot a page, I normally copy the link from personal device and input into MPS aware computer.
		The document is of a large size 14Mb + or blocked as met police believe the council and government websites are unsafe.	There is only one covert open-source terminal in the borough. It is frequently unusable because of connectivity or administration issues (eg no up to date virus software). OSU is an option but it requires quite a bureaucratic form
		The met equipment simply does not work	the MPS blocks sites or links related to PFEW
		pointless trying to do it on work computers.	The aware system would not allow me to see the information I wanted regarding a missing young person. And information is easier to obtain.
Out and about if someone needs a phone number or address for various organisations. Taking photos of a photo of a high risk misper to quickly email to other officers dealing.		The Aware Firewall blocks many sites which have blogs and other types of media incorporated within them. This includes sites attached to University Faculties which house details of research projects related to Policing and criminal justice, even those projects in which the Met are involved.	
Find locations of where someone may be when someone can describe location but does not know address.		MPS Systems are not compatible with Apple. Find My iPhone can't be used but is an excellent tool.	
On occasions when we happen upon a licensing issue whilst out and about. To access the local authority licensing register to view current licenses and licence conditions.		Every person (nearly) has access to a smart device with internet access. It is ridiculous to not use a tool that has access to a wealth of all human knowledge that sits in the palm of your hand. It would be preferable not to use my own device (due to personal costs to have it and access services) but it is foolish not to use something that would aid in your day to day work/life.	
Because MPS technology is not up to scratch and going through the Open Source Unit can be so time consuming and pointless, depending on who does the search.	because MPS devices are so restrictive We need to get the job done!		
because i did not have any Met computer while checking information against council register of licences at the premises. this is done regularly as we did request a iPad but refused so we have no option.	because aware terminals are slow and seldom work! Every enquiry gets blocked and I often find it quicker and easier to use my phone.		
Because AWARE does not allow me to watch video footage	Aware terminal very slow and unable to access some websites due to the firewall. It's quicker to use my own device to get directions than anything provided by the Met.		

Thematic Coding	Themes	Respondent Answer	Respondent Answer
What are the phenomena of concern being mentioned?		Q.7.1. If possible, please provide further details of the incident/occasion to help us understand why you used your own device.	
Why – Which Reasons are Provided or Constructed?	Not for Intel	Been to a call where the person needed to contact action fraud. I used my mobile phone to conduct an internet search for the Action Fraud Number.	Royal Mail website does not run (possibly browser issue)
		Varied occasions. Never used for specific criminal investigation or intelligence enquiries.	Mostly it's to find out uncontroversial information (such as directions, finding a newspaper article etc)
		To assist members of public enquiries whilst on foot patrol, maps, quick routes to get to emergency calls,	
	easy/access/speed	Disorder planned and occurring live on periscope. I was unable to access this via the open source terminal.	
		Usually use my own device as I am out of the station and do not have access to an aware terminal or I will have been at the station and there were no free working terminals	MPS devices do not always allow access to certain sites. Completing a form to request someone else accesses the internet on my behalf, then waiting for the result, is archaic. The internet was born almost 25 years ago. It is beyond comprehension that an organisation can be so far behind the times.
		Speed, necessity, ease of use.	I have also used my phone to update a work twitter account due to my phone having a better camera and being faster.
		Quicker, more efficient, sites are not blocked, working away from the office/terminal	its faster, its a better connection, wider access to sites
		Quicker than using work computer	its far quicker to conduct for fast time investigations and having to avoid a second person.
		Performing a specialist role such as forward intelligence makes it necessary, in order to be more effective, to be aware of tensions and consider where target locations for direct action may be.	it quicker, and easier to access
		Purely ease of access as I was logged into something else	It was most convenient. Before teams were given smart phones, aware terminals were pretty temperamental and the quickest way would be to use a personal device.
		nothing else available	It is the 21st century. Why would i waste time making a request when I can do it on my phone which is in my pocket.
		not issued with a MPS device to use on the street	Unless I needed it in an evidential format and for a paper trail for legal reasons there is no way I would bother making an official request. Unless I had been given the training to do it myself.
		not in a police building, on the street	it is quicker when doing admin
		Not been issued with any mobile job device i.e. laptop or PDA capable of this.	I find it easier to update the police twitter account using my own phone than a terminal
		No access to an MPS mobile device to conduct searches for information for members of the public	It is quicker and easier to use than an aware terminal.
		I am in a LIT (intelligence team) so complete research using various social media and internet searches. The open source unit will only complete the more serious or complex research as often the open source unit consists of a single officer on duty. The ability to search should be opened to all officers.	In any case where the material sought is for intelligence rather than evidential purposes. Because I can do a more thorough job and get quicker results doing it myself than sending a request to LIT or the Open Source Unit.
		No access to a portable device - however this has now changed as I have an MPS laptop.	In an case where the material sought is for intelligence rather than evidential purposes. Because I can do a more thorough job and get quicker results doing it myself than sending a request to LIT or the Open Source Unit.
		I have used my personal device because it is convenient to do so. If I am out and mobile conducting enquiries then it is easier to use my own equipment.	If out on patrol when no other device available or if the information was blocked on the internet ie sometimes journey planner is blocked and the fastest route is required to reduce wasted time. Whi is this blocked on Met systems? Who knows but if it isn't restricted personal phone is often faster and easier to use than desk top.
		My own device is powerful, cloaked and far better than anything that the MPS supply.	I have used Google Translate to communicate with a Farsi speaker as Met radios are a joke in terms of connectivity, and the service from official Language Line is abysmal. Not only do you have to wait an age to speak with anyone, once a translator has been located, they, very often, are rubbish, i.e. they are incapable of speaking/speak very poorly the language requested, which is frustrating for the member of the public and makes us - police - look like a joke.
		faster and more effective way of doing getting the information rather than the outdated technology that we have to use	I am response team, and this is the only internet access I have whilst on duty unless back at base.
		Do not have access to a standalone where i work	For speed and convenience. Only 1 open source computer here. The room is locked when nobody is working in that office.
		Job phone had been previously used during course of same tour of duty for same purpose, out of office on live operation deployment and information was required. "	For facebook you have to deal with the authentication bots, it's just quicker on my phone.
		At the time i was unaware of who or how to get it completed properly and requesting it would take longer than just doing it.	few years ago, was quicker, no paper work and needed intel to build the picture.
		As you cannot use police AWARE computers and contacting an Intel team would take to long or unaware of who to contact.	closed groups. anonymity. ease and speed of use. I am not provided with ANY equipment at work capable of doing it. My aware terminal barely lets me book on let alone use it for anything constructive that could help in my job.
		Apps such as vehicle smart not available on met systems. Google maps and location services disabled on met systems	At the time i was unaware of who or how to get it completed properly and requesting it would take longer than just doing it.
			Away from office with no other devices available.
			At hand, ease of access.
	Access is easier and being able to use Firefox etc makes use of external website quicker/better 1) to access sites that are blocked by the MPS 2) to monitor information away form an MPS terminal 3) to make use of anonymisation techniques (VPN or TOR mostly) in order to complete the above.		

Question 8. Are there any specific occasions/reasons for why you have not used the services of the Open Source Unit? If yes, please tick all those that apply.

Table 8. Reasons why the Open Source Unit (OSU) were not used	Frequency
My request to the OSU was rejected	33
Too time consuming to request research through the OSU	226
Research could be carried out via own personal device	166
Research could be carried out via AWARE	260
Research could be carried out via a standalone (Inc. LIT or colleague)	184
Didn't or don't know the remit for the OSU	293
Didn't or don't know how to contact the OSU	263
Didn't or don't know that the OSU is open 24/7	216
Not Applicable	127

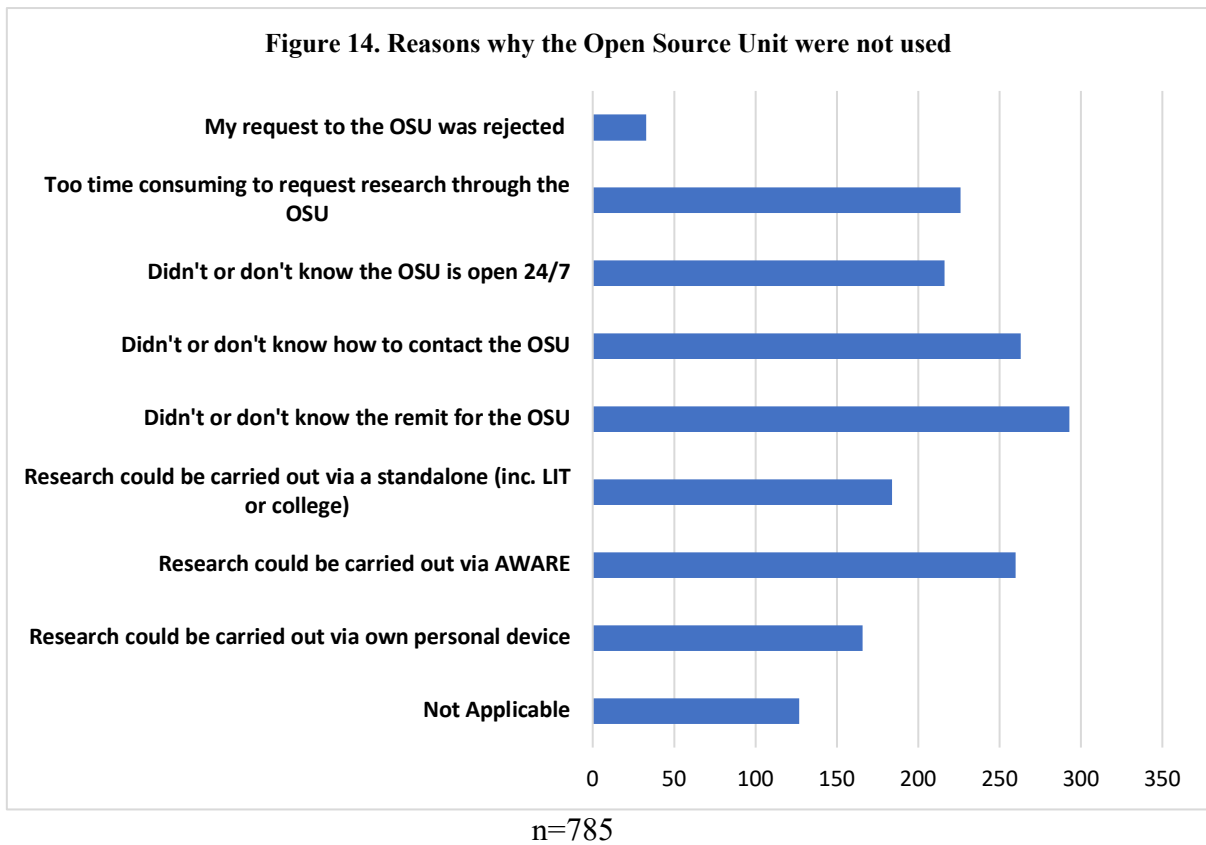


Figure 15. Qualitative Comments and Thematic Coding (Other Comments): Question 8.

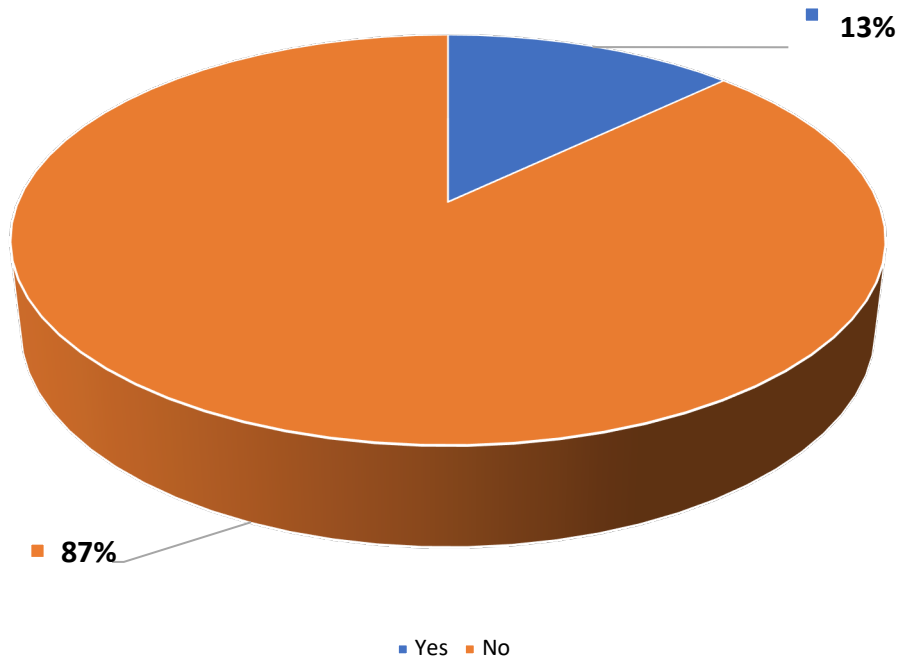
Thematic Coding	Themes	Respondent Answers	
What are the phenomena of concern being mentioned?	Q.8. Are there any specific occasions/reasons why you have not used the services of the Open Source Unit? - Other		
By which – Means/Tactics and strategies for achieving the aim. How are they doing it?	<i>Personal Devices</i>	I've found things on my phone through one quick search that they can't find and it takes them days to reply. A quick enquiry is more easily done on your own device	
Why – Which reasons are provided or constructed?	<i>Bureaucratic</i>	Yet another form to complete and get approval for.	
		Beuracacy of FORM for simple request	
		Far too bureaucratic process	
		bureaucratic process/little staff available/hard to access	
	<i>Should be able to do it myself</i>	Why include them when you can do it now	
		As an OIC I would rather do the work myself and be assured that it has been done to high standard.	
		The requested open source work was not of a such a high priority or urgency that the Open Source Unit had to be involved	
		Requested then did own research in the meantime to save time	
		Prefer to conduct research myself - do not have faith in borough-based PCs to investigate.pointless waste of time for basic inquiries which can be carried out	
		Open source unit do not provide the level of evidential open source work that the SCOIS units require for Murder jobs we are therefore trained to do our own evidential	
		The fact it is open source means it is easily accessible.	
		I can complete this within minutes on my own. In a time pressured environment I'm unwilling to spend time tasking another unit then waiting for results which might not be what I want when they come through	
		Easier to look myself than to brief someone else, especially if I don't know what I'm specifically looking for until I've found it	
		By the time i jhave explained to them what i want i can do it myself ten times over..... We need to get into the modern age. The open source unit is just another central unit that spends more time telling us why they cant do it. Centralise something and we have lost it on the boroughs.	
		pointless waste of time for basic inquiries which can be carried out yourself	
		Tend to use OSU mostly when the product may be required evidentially, when it is "not safe" to do myself, or also when I have been unable to locate the desired data	
		<i>Efficient</i>	Sometimes the information needed quickly. Has been multiple occasions where local LIT have failed to identify images/information on suspects that I've managed to find on my personal device.
			Research could not be carried out via MPS terminals and the open source unit invariably reply saying they couldn't find what I was looking for.
	complete forms and await results several days later in previous delaings/requersts.		
	Open source unit do not do evidential work they only provide a quick snapshot		
	Not operationally effective to continually make requests , information required at that point.		
	<i>Poor Standards</i>	In many of my investigations, the information gleaned from one search will then lead onto another relevant area which another person would not realise this and not perform the additional searches; this is probably the most important reason why i do the searches myself and not trust them to another officer.	
		Open source isn't completed to my standards by other departments. if you want it done properly you have to do it- other faceless departments aren't motivated to do it	
		Not trusting of the results and would prefer to conduct them myself	
		I have had requests processed by the Open Source Unit before, and the infomation they have obtained was not of a satisfactory standard.	
	<i>Time Consuming</i>	I am already adept at conducting open source reasearch, and the work I have received from	
		Open Source in the past has been sub-standard and missed obvious things I have later found myself with minimal effort. Having a dedicated unit to conduct internet research when each officer has access to the internet seems like a poor use of	
		Thought it would take a long time to get the result	
Required fast time and not able to be completed quickly			
<i>Didn't know they exist</i>	OSU unable to assist quicktime due to workload		
	Open source unit doesnt work fast enough for fast time manhunts		
	Was unaware that the Open Source Unit existed		
	I do not know what an open source unit is.		

Question 9. Have you ever used your personal social media account (Facebook etc) to conduct Online Investigation (Open Source) research?

Table 9.

Used Personal Social Media for Research?	Frequency	Percentage
Yes	101	13
No	684	87

Figure 16. Have you ever used your personal social media account (Facebook, etc) to conduct Online Investigations (Open Source) research?



n=785.

Figure 17. Qualitative Comments and Thematic Coding: Question 9.

Thematic Coding	Themes	Respondent Answers	Respondent Answers
What are the phenomena of concern being mentioned?	Q.9 Have you ever used your personal social media account (Facebook etc) to conduct Internet Investigation & Research (Open Source research) - [Comment]		
Why – Which reasons are provided or constructed?	You're Kidding	You're kidding, right?!	I'd rather not have a link to suspects on social media. The algorithms on social media sites are too smart and will see that you've searched for suspects.
		Wouldn't be so daft...	Considering some of the suspects I go after this would be very dangerous
		Surely this is a breach of data protection standards and MPS	Because that is insane
		No as there can be trace which would link my personal account to having searched for the suspect and facebook may then use that data to link me to the subject and he would then be able to find me despite my high security settings.	Please note, I would not do this in cases involving anyone likely to realise what was going on
		No however I have frequently seen others do so.	It is my understanding that we are prohibited from doing this due to security issues.
	Efficiency	You have to fill out a form, it's too long lengthy and time consuming, you have to wait in the queue as there are things more urgent than your enquiry	Easier than having to go through open source unit - Fast time intelligence is required and do not have time to submit a form
		Whilst at court it had been suggested that victim had used facebook. Needed to complete search at the time.	easier and time efficient
		Quickest and easiest way to conduct fast time enquiry.	Because although it is against the policy - its often much easier and quicker than using a standalone. if the subjects being looked at are not organised criminals etc and would not have the ability to see who is looking at them I have research them on my personal accounts
		Easier, quicker and more effective than tasking OSU.	

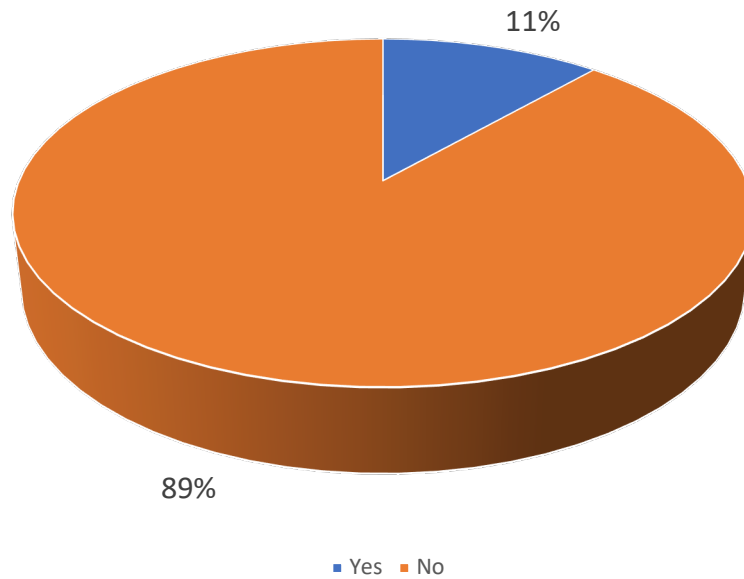
Thematic Coding	Themes	Respondent Answers	Respondent Answers	
What are the phenomena of concern being mentioned?	Q.9 Have you ever used your personal social media account (Facebook etc.) to conduct Internet investigation & Research (Open Source research) - [Comment]			
Why – Which reasons are provided or constructed? (Continued)	Safeguarding	To see if there were recent updates by missing persons.	Misper enquiry to see if subject is on FB.	
		To see if a missing person has a facebook page and if any messages status updates have been added	I used instagram to help with a missing person investigation. I have since been told this is not advisable.	
		To see if a misper had posted that day	I cannot remember specifically but have used my private social media accounts to see if mispers have social media accounts and if any information is useful	
		To search for relatives listed on a victim's facebook page who was in a coma. Trying to urgently ID NOK details.	Looking at advertised events and known organisers to look for Intels which will assist us in planning. Eg High risk of public disorder, community tensions on particular events etc	
		I created after concerns were identified during an encounter between a Mother, her new boyfriend and the Mother's 12 year old daughter	As part of my License Enforcement Officer role	
		To locate high risk Misper	As above for high risk mispers. Normally stating they are going to commit suicide and I want to see if they are on social media, exactly what is being posted. I can also see if they are posting anything else which will assist me with assessing the risk.	
		A very high risk missing person I looked at personal account which assisted in finding MISPER in quick time		
	Access to IT	When on borough didn't have access to stand alone and the investigation was time critical		
	Intelligence Purposes	WhatsApp - by adding a SUSP's number to phone via number provided, we were able to obtain an image of them, as they had their photo as their profile photo. They cannot tell that we have added them just by our saving their phone number to our mobile phone	Facebook searches for suspects' profiles for information and intelligence "	
		Twitter and Facebook to identify local crime.	Searching for names of potential suspects to determine if they exist. I would NEVER add them or interact (direct messaging etc)	
		Twitter - unintentionally saw a retweet in twitter feed of a gang nominal video which resulted in intelligence.	searched people on instagram such as 'Duckfeddaily' or other anti police accounts. Some members or posts are gang members	
		To try to identify a subjects Facebook/Instagram account to obtain an up to date photograph of them.	Searched names to see a face or obtain further information. (domestics, Mispers ect)	
		To track down a female involved in tenancy fraud	Searched for suspect who was wanted	
		To search for other users on Instagram, and to view their accounts, you yourself need to be logged into an account.	Running searches for names etc. to see if they have a social media account.	
		To search for a person / mobile number on facebook etc	Read-only to monitor closed social media groups, with locations fo dumped stolen vehicles to enable me to recover them back to R/K. Can't be viewed from aware/met terminals	
		I use PIPL.com"	Only to look at a suspect's photo	
		To search a person for profile picture	I was asked by a supervisor to look for a suspect on Instagram - as this is an app that one must have an account to use I obliged.	
		To search a name for a suspect	I maintain a simple 'dummy' Facebook account to use for research. I am aware that I cannot interact with others using this account	
		To look for suspects	I have used Twitter in an attempt to locate a suspect and also to research a victim	
		To look for stolen bike sales	I have a fake account that I use for work just like many other investigators have had to do.	
		To look at the relationships and profiles between family members following on from a Merlin	I have a fake account that I use as it is the only way to get the job done without filling out loads of forms.	
		To identify location of an organised event where no risk to self.	For example searching telephone numbers to link to an account name	
		Searching for organised crime suspects and associates	I wanted quick research conducted on potential drug dealer. Wanted latest pictures of him he may have on facebook,	
		Check up on CCTV clips that have been posted on residents groups and not submitted to police	Downloaded several Gang Videos from You Tube, as request for Met Intel - had not been done some 2 weeks later,	
		Carry out research on youth and their trends	Confirm identity of an individual.	
		By joining open groups to be kept informed of information.	Conducted searches for profiles of known offenders	
		I do know people that have because during fast time man hunt have used the log in section (forgotten login details) to search telephone numbers and names	Acertain names of Gang Nominals Just to check a photo or email address of a victim.	
		No Reason Provided	Used Facebook account to search for suspect's Facebook account	Looked to see if someone had a Facebook account
			Searched Facebook	Looked on Facebook to confirm identity of subjects and connections to their friends
			Searched Twitter x 2	I have used colleagues as not on facebook
			Through facebook/ instagram apps.	I have created an account for just such purposes.
	I did not establish contact via my personal device as my own personal account should not be used when representing the MPS.		Searching a name on facebook and looking at a profile picture of an open account and linked friends (only if the account is unrestricted)	
	Only search facilities			
	Communication /Engagement	Sent messages on IM to members of the public who have lost their property, usually a wallet or purse/handbag.	Look for members of public's friends when their phone ran out of battery in order to get in contact with them.	
		Only to see if they had a facebook account. I then made a request through media and com's to contact the subject so they could meet with me to collect paperwork from a court which had to be signed for (current address was unknown - not a criminal matter). request was refused by media and comms.	finding a wallet in public I could use Facebook to track down the owner and reunite them with it.	
		Once, in 2009, when all efforts to contact a key witness had failed. Set up a facebook account in my name and found the witness and contacted her directly. This resulted in her giving evidence via live link from Hungary	By joining open groups to be kept informed of information.	
		Ask members of the public to contact police as witnesses to incidents		

Question 10. Have you used a false persona (assumed identity to mask your own) to conduct Online Investigation (Open Source) searches/research?

Table 10.

Have you used a false persona	Frequency	Percentage
Yes	90	11
No	695	89

Figure 18. Have you used a false persona to conduct Online Investigation (Open Source) searches/research?



n=785.

Table 11. Frequency of False Persona use at each Open Source Level

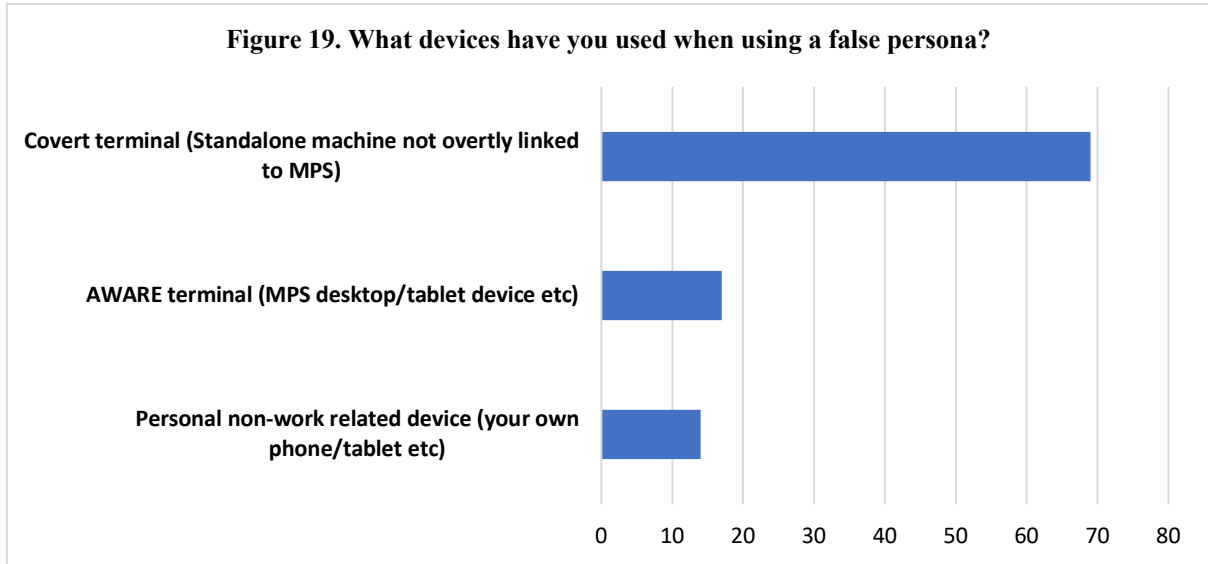
Open Source Levels	Frequency	Using False Personas Frequency	Percentages
Level 1	685	24	3.5
Level 2	78	48	61.5
Level 3	16	13	81.3
Level 4	1	1	100
Level 5	5	4	80
	Total	90	

Question 10.1. (If yes to Q.10)

What device(s) have you used when using a false persona? Please tick all that apply.

Table 12.

Devices Used	Frequency
Personal non-work-related device (your own phone/tablet etc)	14
AWARE terminal (MPS desktop/tablet device etc)	17
Covert terminal (Standalone machine not overtly linked to MPS)	69



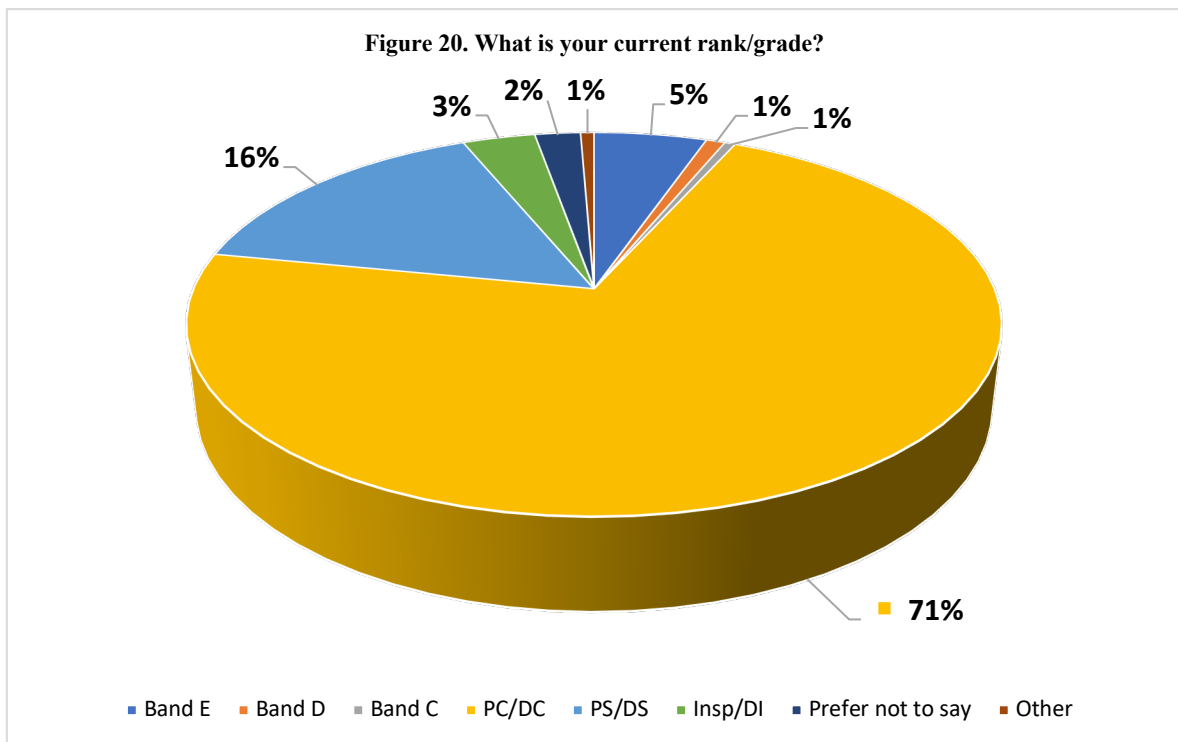
n=90, modal response – Covert Terminal (69).

Demographic Questions

Question 15. What your current rank/grade is?

Table 13.

Position	Frequency	Percentage
Band E	42	5
Band D	7	1
Band C	4	1
PC/DC	560	71
PS/DS	123	16
Insp/DI	27	3
Prefer not to say	17	2
Other	5	1

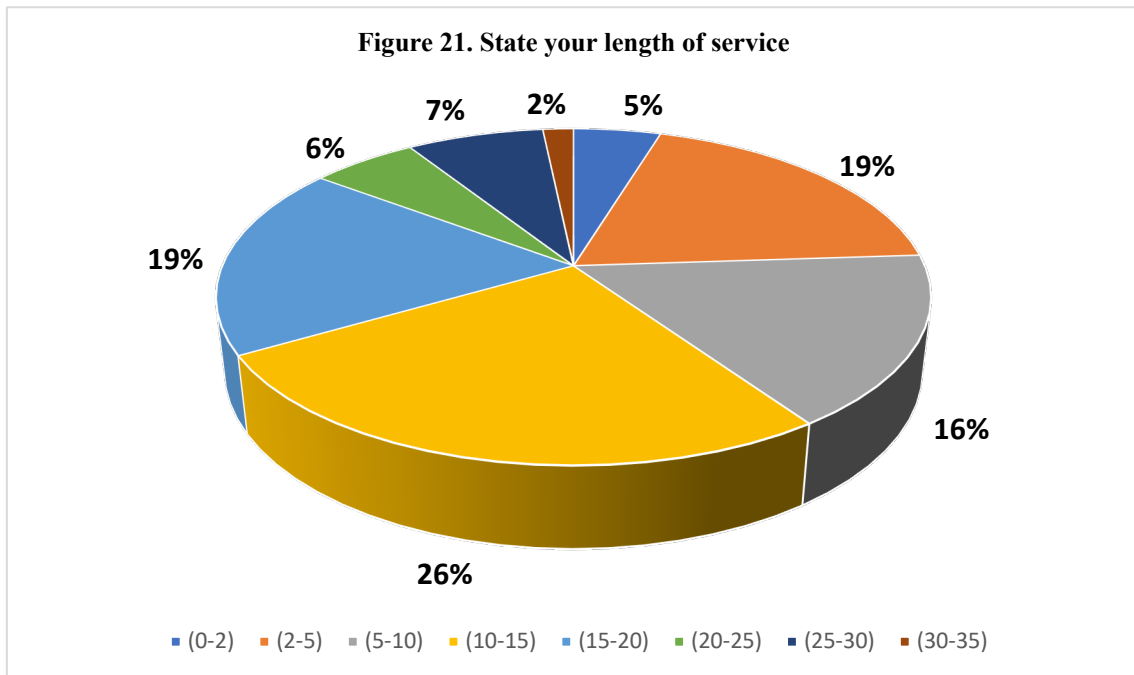


n=785, modal response – PC/DC (560).

Question 16. Please state your length of service.

Table 14.

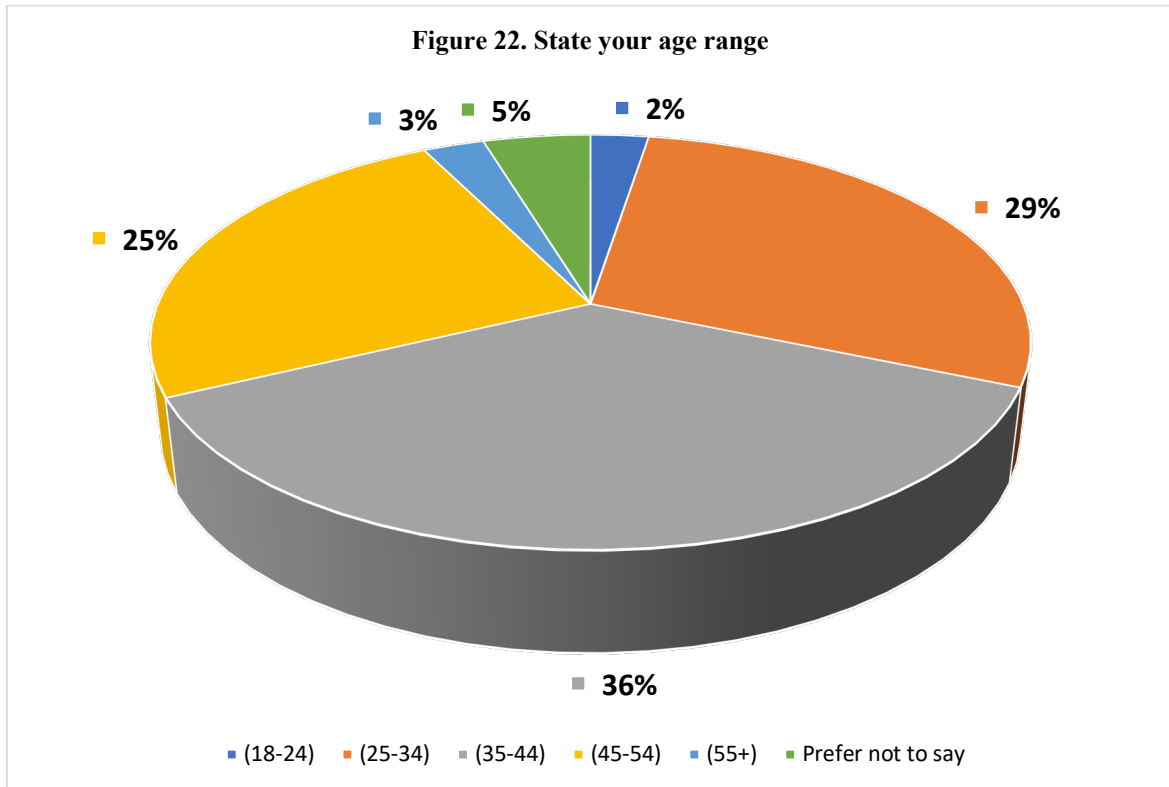
Length of service (years)	Frequency	Percentage
0-2 years	37	5
2-5 years	151	19
5-10 years	129	16
10-15 years	206	26
15-20 years	146	19
20-25 years	45	6
25-30 years	58	7
30-35 years	13	2



Question 17. Please select your age group.

Table 15.

Age Range	Frequency	Percentage
18-24	20	2
25-34	226	29
35-44	287	36
45-54	194	25
55+	21	3
Prefer not to say	37	5



n=785, modal response – 35-44 (287).

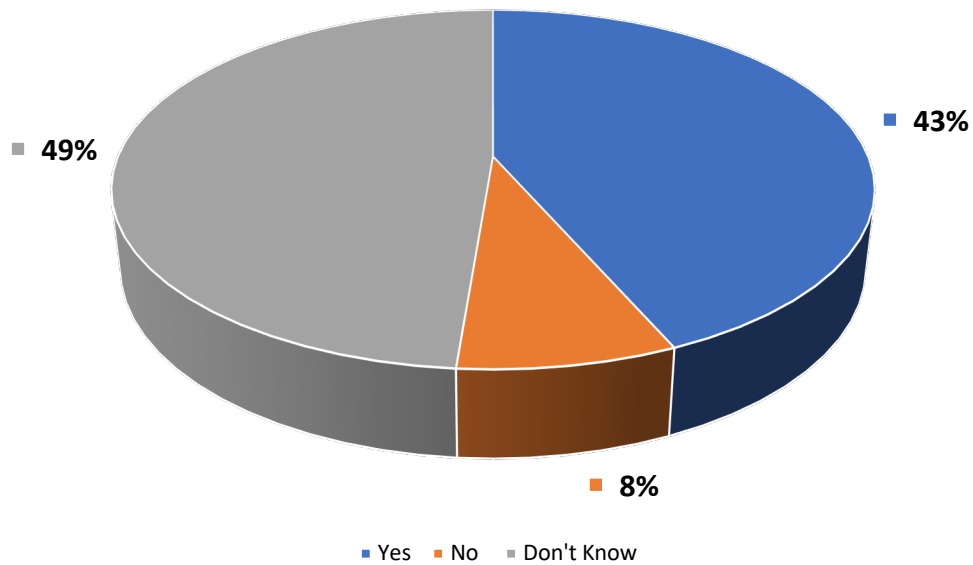
Knowledge Based Questions

Question 1. Does the Regulation of Investigatory Powers Act (RIPA 2000) impact the way in which police obtain Online Investigation (Open Source) intelligence?

Table 16.

Does RIPA Impacts obtaining OS Intelligence	Frequency	Percentage
Yes	271	43
No	49	8
Don't Know	304	49

Figure 23. Does the Regulation of Investigatory Powers Act (2000) impact the way in which police obtain Internet Investigation and Research (Open Source) intelligence?



n=624, modal response – Don't Know.

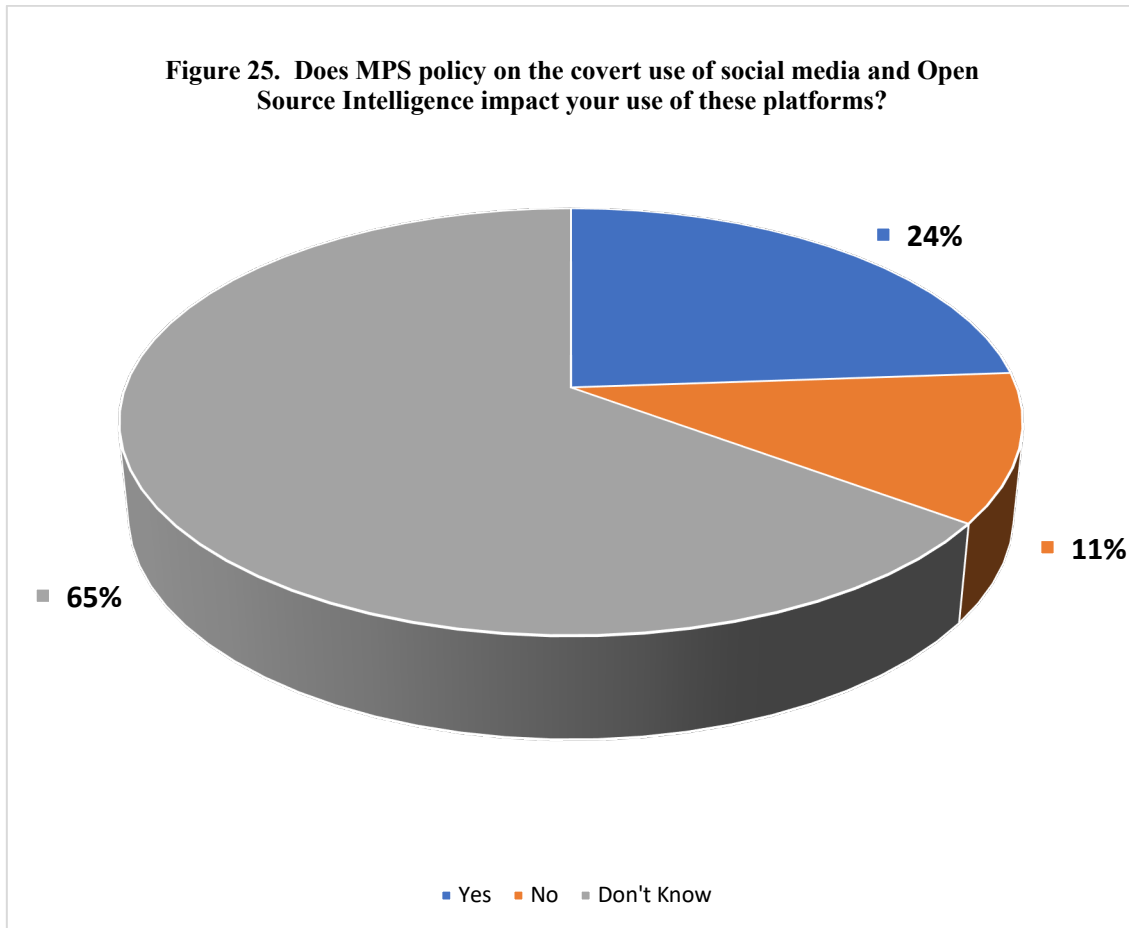
Figure 24. Qualitative Comments and Thematic Coding: Question 1.

Thematic Coding	Themes	Participant Response	Participant Response
What are the phenomena of concern being mentioned?	Q.1 Knowledge Section - Does the Regulation of Investigatory Powers Act (RIPA 2000) impact the way in which police obtain Internet investigation & Research (Open Source) intelligence- [Comment]		
Why - Which reasons are provided or constructed?	Repeat Viewing	Yes repeated viewing is considered surveillance and clearly we cannot create fake profiles or risk being deemed a CHS/UC. Even where there is no contact between police profile and person of interest.	It does because we cannot look at someone's public posts on a regular basis without breaching RIPA. If they are posting things online there is an expectation that this is public. Unless you are an online UC.
		Viewing profiles repeatedly - for a specific operation requires in my opinion a Directed Surveillance Authority.	It does affect it if open source is being used constantly (refreshed) hourly or daily. It could cause an issue in court with regards if this needs to be covered under RIPA for directed surveillance. We are following the suspects digital footprint. It details how we can monitor suspects internet accounts that are password
		Some material that can be obtained from the internet (especially social networking profiles) can be considered private information and will be directed surveillance if repeatedly/frequently viewed.	It can. An example would be repeated access to a subjects facebook account which would start to get into the realms of surveillance.
		RIPA is for covert and intrusive surveillance. Simply viewing open source material on the internet does not require RIPA authority as long as you are not constantly monitoring it.	Information obtained can only be obtained from what is already there ie a Facebook profile. A DS authority will be required if profiles are actively monitored or friend requests/relationships are made.
		Ripa is always considered in the work I do with repeat viewings of social media etc. some of the work can be classed as surveillance and again Ripa would apply	If you repeatedly look at Social Media postings to gather intelligence then you need to be aware of collateral damage ie finding out stuff about friends etc that are not relevant to your investigation.
		RIPA - with regards Social media researchOne off research is fine. However, looking at an account more than once can be deemed "monitoring" and should be authorised as Directed Surveillance	If you are regularly checking someones face book account or other social media accounts you're likely to be obtaining private/personal information and experiencing collateral with regards to others commenting on the items being posted/commented on and therefore potentially breaching RIPA.
		Repeated covert viewing requires a DSA	I believe it relates to the overt or covert use of the systems and whether you are merely checking sites or continually monitoring someones usage of something which could amount to surveillance.
		Repeated searches of specific social media profiles requires Directed Surveillance Authority	You are restricted by the amount of times you can look into a subjects details without impacting on RIPA
		Repeated viewing and ongoing monitoring, you are able to access an account once however if you are wishing to monitor an account for updates or daily posts this would	You cannot complete repeated viewing without a DSA in place - which is ridiculous as its all in the public domain !!!
		Ongoing consistent viewing of a subjects social media profile may breach RIPA	You can look on open source for investigation purposes, but if you wish to repeatedly look at someone's profile you would need a DSA due to human rights and privacy.
	RIPA and this includes repetitive viewing of what are deemed to be "open source" sites for the purpose of intelligence gathering and data collation."		
	Open Source Not Subject to RIPA	Open Source is not subject to RIPA	No its not targeted covert surveillance, its accessing historically public
		Open source = open to the public	No as the surveillance is not covert.
		Open source doesn't count as surveillance	Material found through 'open source' is open to all. There are no covert methods being used and the material is available for anyone to access.
		Non-contact research, however, is ok without RIPA application.	As stated, RIPA was legislated before Social media took off, the current view is outdated and public profiles should not be come under RIPA in any form, even with repeated viewing they are public and anyone can view them. Journalists/MOP/Business can do this repeatedly but because we are police we cannot.
		Not if the information is readily available on the internet and without interaction. If the information is available on a public domain, I do not believe RIPA is in use.	No, because it is not private information.
	Open Source is not Private Information	No, everything online is accessible to anyone. Anything gained has not been gained by obtrusive methods.	"No. If its publicly available it has been disseminated for public consumption. It is covert gathering of information for a policing purpose and it would be directed with a risk of collateral intrusion so it does fall within the RIPA definition but the fact that is in a public domain, there is a tacit agreement that it can be looked at. However, if the information is restricted in some way then RIPA would apply. The main issue with open source is not to leave a footprint."
		Open source is publicly available and although covert it is not accessing private information.	Although information on social media accounts such as private communications within platforms is protected by RIPA most public posts are not covered
		This is information open to the public. The owners of the data can have no expectation that the data is 'private' Accessing the account information would likely be subject to restrictions but the purpose of Open Source is to complete research on publicly available information	Anything in the public world, we as police should be able to use it without the fear of breaching any act or policy. Suspect has been involved in crime on a particular date, people are so flash with the latest phone and take selfies, this may prove the clothing worn and the suspects features.
	Proportionality/Necessity/Collateral Intrusion	Obtaining private information about suspects must be justified and proportionate not too familiar with RIPA act	for events in your area and names come up, it would not, but if these names are then specifically looked into at this point it may and must be
	Online V's Real Life	Online interactions are governed in the same way as real-life interactions and the same legislation applies	Of course it does. The same rules apply to establishing and maintaining a relationship for a covert purpose as they do to UC and CHS tasking.
	Not Sure	Not sure but would guess at yes as if we are tracking someone online then technically we are following them and keeping them under observation. Not certain, but I'm guessing that simply viewing overtly visible information doesn't need authorisation, or making overt contact through social media from a police account, while establishing contact using any sort of anonymous account would need RIPA authorisation.	make that "yes, probably". Though I find myself wondering if we over-think it. Most of our interest is from an Intelligence Only viewpoint and not needed for investigations. It's a grey area for me - but I would have thought there would be restrictions of some kind with certain searches
		Many officers are not clear on when or if they need an authority or what the authority required actually is.	Again, on the brothel investigation I wanted to do some covert surveillance and watch the comings and goings but had to take advice from line managers whether a RIPA was needed. Nobody could really answer the question so I googled it myself .
Policing Purpose	No. If its publicly available it has been disseminated for public consumption. It is covert gathering of information for a policing purpose and it would be directed with a risk of collateral intrusion so it does fall within the RIPA definition but the fact that is in a public domain, there is a tacit agreement that it can be looked at. However, if the information is restricted in some way then RIPA would apply. The main issue with open source is not to leave a footprint.		

Question 2. Does MPS Policy on the covert use of Social Media and Open Source Intelligence impact your use of these platforms?

Table 17.

Does MPS Policy obtaining OS Intelligence?	Frequency	Percentage
Yes	149	24
No	70	11
Don't Know	405	65

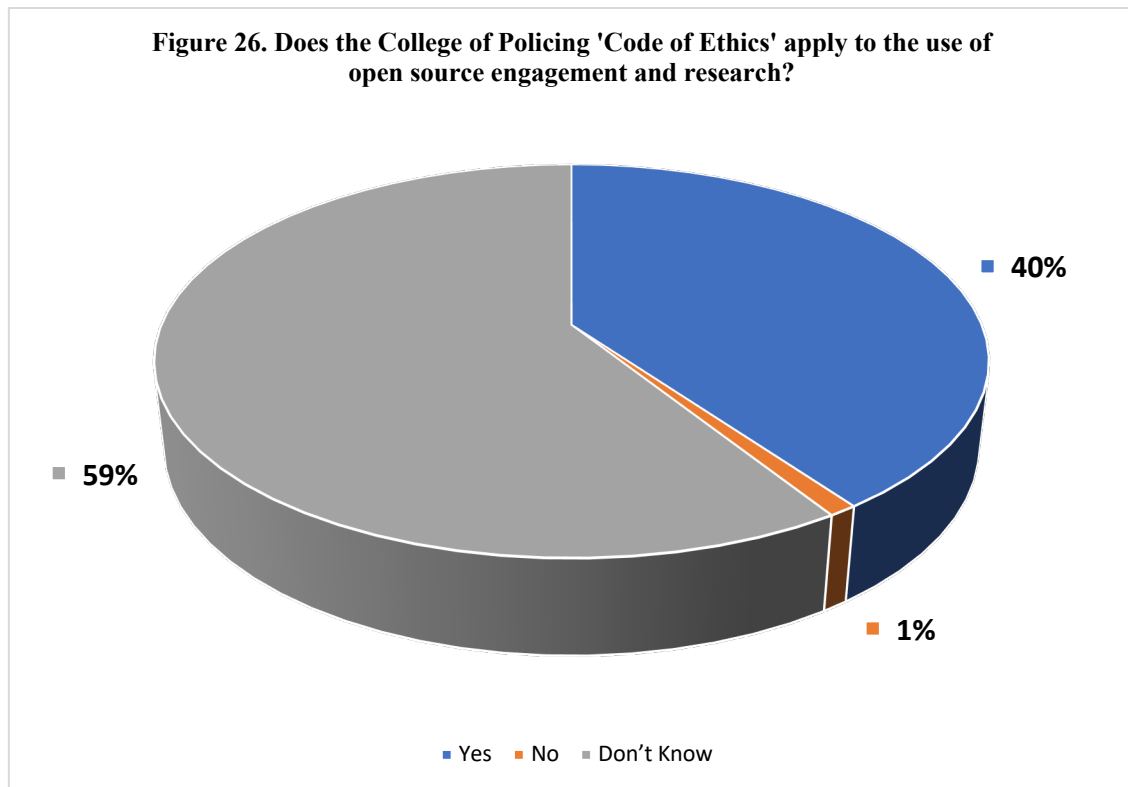


n=624, modal response – Don't Know (405).

Question 3. Does the College of Policing 'Code of Ethics' apply to the use of open source engagement and research?

Table 18.

Does the Code of Ethics apply to the use of Open Source?	Frequency	Percentage
Yes	250	40
No	6	1
Don't Know	368	59

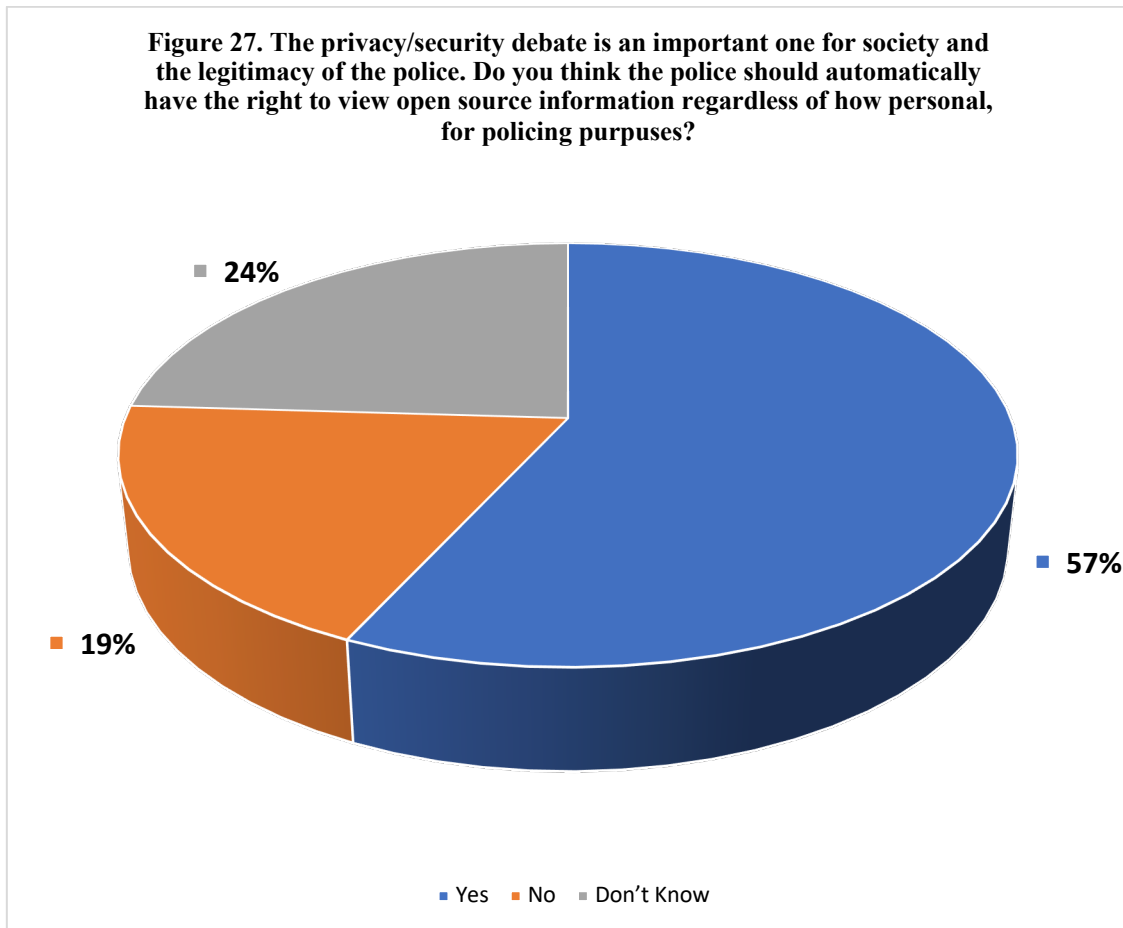


n=624 modal response – Don't Know (368).

Question 4. The privacy/security debate is an important one for society and the legitimacy of the police. Do you think the police should automatically have the right to view open source information regardless of how personal, for a policing purpose?

Table 19.

Do the police have the right to automatically view open source information regardless how personal?	Frequency	Percentage
Yes	355	57
No	119	19
Don't Know	150	24



n=624, modal response – Yes (355).

Figure 28. Qualitative Comments and Thematic Coding: Question 4.

Thematic Coding	Themes	Respondent Answers	Respondent Answers	Respondent Answers
What are the phenomena of concern being mentioned?	Q.4 Knowledge Section - The privacy/security debate is an important one for society and the legitimacy of the police. Do you think the police should automatically have the right to view open source information regardless of how personal, for policing purposes- [Comment]			
Why – Which reasons provided or constructed?	Yes - Access should be automatic	Yes. It is a shocking idea, but if anyone is uploading information on networks which could in theory be accessed by any good hacker, then the subject knows that the information should get in anyone's hand and the Police should have automatic right to view it to protect children and vulnerable people, among other things.	Yes, providing it is auditable and regulated. Like phone work; applications would be an appropriate hurdle. I don't think a blanket access is necessary except in exceptional circumstances - terrorism etc.	If the same information would be available to any person searching the internet (ie: privacy settings, facebook accounts etc) then it should be able to be used legitimately by the police without restraint... perhaps it is, my knowledge on the subject is minimal now, although I am under the impression it cannot be? However, the accessing of information which would otherwise be private to any person, should require necessary authorities.
		I can't decide on this - the police officer in me would say a big yes - as a private person I would have concerns about an unquestionable right to delve into people's lives	If it can be seen on the internet then we should have access to use it as evidence, but maybe it needs to be treated a bit like hearsay evidence.	If the open source info is viewable by any person in whatever format I believe the police should be able to view that unhindered for policing purposes. If it requires hacking or by passing of security then I believe there needs to be a level of authority attached to this.
		Yes. In some cases, results of open source research may provide specific information that may not have been available on commonly used police indices	Yes as long as there is a legitimate reason if that reason protects others.	If the Police believe the information would progress any type of investigation then it should be permitted to access the relevant information
		If any member of the public can view it on a personal device why should the Police not also use it when available?	I think if anyone makes any information/images/text public, police should be able to view it as easily as a member of the public can. Furthermore, police should be able to record and use this information in the evidential chain easier.	If the subject is putting it on social media for the world to see, the police have a right to view it.
		Yes. If we can view it openly then it cannot be that personal.	Yes, if it's in the public domain it seems fair i.e. it has been consciously put on the internet by the individual concerned.	If someone is under investigation for a crime then yes. We need to prove guilt and obtain facts to build a case against a suspect.
		I'm not sure I understand the question. If you mean information that's in the public domain then it seems a bit odd to suggest police should artificially act as though it's not. If it means social media details secured using privacy settings, then the same restrictions should apply as for other private data.	yes if this for policing issues	If people put it in the public domain we should be able to use it, the media etc can. It would make people think twice about posting things online.
		Yes, within the right parameters	Whatever it takes to catch criminals.	If someone has published personal material about themselves they have effectively forfeited any right to privacy.
		I think people would be prepared to accept this.	Yes if there is an urgent investigation which could be assisted fast time by having the right to view it	IF PEOPLE KNEW THAT WE COULD DO THIS THEN MAYBE CRIME WOULD DROP
		If there is a policing purpose, police should have the same rights as anybody else to look at publicly available data / information. There are enough privacy settings on social media so that users can set them to prevent unwanted intrusion. I think the same celebrity debate as public life vs private life can be applied here. If the user chooses to broadcast themselves in whatever manner then it becomes their responsibility to manage private data and ensure what they are putting up is legal and morale. Public morality is driven by public oversight. It does shift but it is gradual. It is a publicly vital concept as public morality will drive changes in law such as gender equality and sexuality. It is dependent on the individual thought processes that drive current thinking facilitated as rights in our society as democratic principles of free speech and Humanitarian law (freedom of association for etc.). Law enforcement agencies have a crucial part to play in the establishment of public morality as they are not just punitive, but are the principle challengers to public thinking, ultimately by judicial process. if you consider that law arises from public morality then police enforce those laws and challenge any action and thereby thinking that has been deemed by common law and statute as unlawful. There must thus be a tacit understanding and thus permission by members of the public that broadcast on public platforms that what they put out in the public domain may be tested. Online opinion is a major factor in public campaigns and just because public morality has effectively "gone online" which permits the far wider dissemination of individual information and views. It is a fundamental requirement in society that this information / view point is tested where appropriate. Just because there is a certain remoteness to online activities does not change the fact that an individual is not remote from public morality and due process. The fundamental paper principle of "caveat subscriptor" (let the signor beware) must equally apply to online activities. If an individual does not privatise his or her information then there must be an understanding that it is in the public domain and subject to use by whoever views it, including law enforcement agencies.	Yes because if it's "open source" then that means it's publicly available. We're not talking about interception of communications here. It would be stupid not to be able to access information that my son could get on his mobile phone..	If someone has posted information publicly, they are making it available to anyone, including friends, family, strangers, police, journalists, politicians, etc. Therefore, one cannot be surprised if someone finds that information. However, if someone makes efforts to make the information less public (ie viewable by friends and family only), then it should be expected that police should have to gain authority in order to access that information. Equally, police should not trawl the internet for potential offences, but if a crime has been reported, it would be inappropriate to exclude or neglect publicly available open source material. It would certainly be of benefit for everyone, especially teenagers, to be better educated in the implications of making information public, so that they can decide for themselves what they are happy to share.
		Yes 100%. Surely we should at least have the same access as member of the public. I think we should have dummy accounts that could benefit the Police from conducting necessary real time policing. Surely not having open access is not letting Police conduct their own proactive investigations.	Yes definitely. Social media is ubiquitous and is used in various ways by the criminal fraternity. It would be more than likely that personal information would be contained within most peoples social media profiles and there would be to some extent collateral intrusion. As with any other powers that police are afforded there would obviously need to be accountability and real reason for viewing open source material.	If people willingly create a social media profile and content that the whole world can see they're surely consenting to everyone, regardless of who they are, viewing it.
		That information could be the key reason why person is found guilty/not guilty. Information obtained that way often assists in	Police should look into anyone committing crime and the courts should hand down heavy punishments to	If people put it out there for others to see then they should be happy for anyone to see it!
		Surely it being open source suggests anyone can access it. Why should police be any different?	Why put obstacles in the way	If its for policing purposes we should have all the access we need; not only would greater access keep people safer and bring more offenders to justice it would improve the efficiency of the police by removing some of the hoops we have to jump through

Figure 28. Qualitative Comments and Thematic Coding: Question 4.

Thematic Coding	Themes	Respondent Answers	Respondent Answers	Respondent Answers
What are the phenomena of concern being mentioned?	Q.4 Knowledge Section - The privacy/security debate is an important one for society and the legitimacy of the police. Do you think the police should automatically have the right to view open source information regardless of how personal, for policing purposes- [Comment]			
Why – Reasons provided or constructed?	Yes - Access should be automatic	information placed freely online can be viewed by anyone around the world. There would be no reason to exclude police from this community - indeed we could face criticism if we chose to not view that which is free for everyone else to see. Society and legislation requires us to protect the vulnerable as well as prevent crime - we should vigorously contest any efforts to curb our capabilities in these areas. If the communities we serve have an online presence, then we should also be capable of protecting them in that space and be able to act against anyone who commits crime in this space or whose use of this space gives us an window to act against their 'real world' offending.	We need to react quickly to events. The police don't care about what you find embarrassing, we don't come into work thinking 'I cant wait to view someone's personal info'. The culture of today is quick to restrict officers in doing their job effectively, but even quicker to condemn or criticise if we don't get certain information quickly. The nature of the world has changed, data is an important revenue stream so peoples data will be online or stored securely on websites. If we need to access it, it should be given quickly. Again, we don't come into work thinking how can i snoop on someone for the sake of it.	I believe that the internet can be used for more sinister purposes, if you have nothing to hide you have nothing to worry about, this is another reason why I don't have social media other than one application on my personal phone as I have nothing to hide , however I do not understand social media enough and I do not want to. I am happy for the source unit to look at and develop information for the purposes of covert policing, this way errors can be avoided in how we obtain this information.
		Yes - if you want privacy you shouldn't be using social media, the idea that you can "connect" with the world but retain absolute privacy is childish. Criminals are becoming aware of our restrictions and are openly exploiting the fact we need such high levels of authority.	We have to be able to safely view everything that's out there	If it's public - the person has decided it's permissible for anyone (including the police) to view. We can look for people in public (and legally take their photo / film them) with no legal concerns (at least in terms of copyright / permission). Applying surveillance on social media accounts and recording all posted i suppose would be much the same as a real-world investigation and duly require RIPA authority in the same way.
		To be honest, we have a lot more freedom in the UK than al lot of places around the world, i think the price of having freedom to be online and indeed living as a citizen here in the UK, the people should be subject to the authorities, and people should be open to scrutiny just as the Police and the authorities are. This is the cost of national safety. Sadly in this day and age, we forget that sometimes we have to forgo the rights and privileges we all enjoy and take for granted for the greater good, to keep everyone safe.	We are the Police at the end of the day. We should be able to access whatever we want whenever we want as long as its for a work purpose, there should be zero restrictions. People and human rights activists wont like that but its tough, if you want your country to be	I believe that if something is in the public arena it is fair to access, record and utilise it. If the public have chosen privacy controls then these should be respected however the confidence and ability of the police to access and gather information should not be impeded beyond what would apply to a normal member of the public. An example would be where an investigation has failed due to these limitations. We are then professionally embarrassed by a journalist who doesn't have to conform to the same standards.
		There are rights - 'public' info is fair game but things that are set private or only to friends/family, etc. is just the same as 'private' conversations in your home - as such that should need 'powers' to look at	Policing purposes would mean that there should be a legitimate reason. Often not having automatic rights can be a hindrance and slow down investigations and crime reports. For example in a case of harassment, malicious communications an automatic access to facebook would be helpful and a more efficient way to proceed with some investigations.	GDPR I would say is one of the bigger concerns in this (applying from early-mid 2018). RIPA perhaps less so, as looking at someone's public persona is completely fine. Recording it is the difference, so if the MPS are not recording what they see on the individual's personal social media, then there is no issue (although this risks the integrity of the investigation being harmed, as the user may just delete the information and it will be lost, undermining potential evidence)."
		By its nature open source information is public.	This could help identify and link priority outstanding offenders	If it's publicly available then we should - it would just be ridiculous if we had to jump through hoops to get information that any private individual could get hold of in 5 minutes - potentially make us look daft at court!
		Open-source is freely available data; if someone sticks personal information about themselves on the side of their house it is equally freely available.	Policing purposes are there to save life and limb, investigate crime and protect vulnerable individuals. These purposes should not be impeded by people views on privacy.	If it's out there then anyone or any organisation can see it. MoP's have implicitly consented so we should be able to fill our boots as long as there is a legitimate policing purpose.
		Open source, which is available to all, should be available to police and public alike. If it is not open source, eg private Facebook account open source yes; if public can access it then so should Police.	Open source = Public. We are duty bound to investigate without fear or favour, if it's out there and ultimately the data any of us post on social media is published voluntarily.	If it's open source then by its very nature it's available for all to view
		open source should be used for policing purposes. It's on the internet anyway, why not use it?	Of course. The public know everyone can see what they are doing.	If it's open and freely available then why shouldn't the Police access it.
		Open source means just that. Material posted onto a public forum	In order to further help and deal with investigations but only through a covert office as it is being currently done.	I believe the individual is responsible for protecting their own privacy on social media, assuming that they are given the opportunity to easily do so.
		Open source material is there to use otherwise the police have less powers than members of the public .	Of course we should, if everyone else can why not the police?	I believe that if someone has posted something on an open format on the internet such as facebook or other social media site then police should be able to access this.
		Open source is, by definition, available to all. It is ridiculous to suggest the police would not be able to look at information that the victim of a crime could legally and legitimately find in seconds.	This can be used to find missing people, family of deceased people, people wanted for offences (serious or otherwise), intelligence for vehicles used by subject in crime, connections with other criminals,	I believe that the duty we have to preserve and protect life outweighs all other rights
		Open source is available to all... Police are not using any powers to access it so I see no reason why not?	It could have a very detrimental effect on the outcome of a case if the information is not made readily available	I am a firm believer that we should have access to any/all systems and that this should all start from a National Identity Card which should be introduced.
		open source is available for all so therefore should be available for police to use.	Information is placed on a public domain for any person to view	I feel this would speed up investigation time to find outstanding suspects
		Open source information is published for all to see, including the police, it is similar to walking down the street waving a banner. There are privacy options that people may use if they wish to keep information to a relative level of privacy.	This could assist the investigation so if it's for policing purposes we should be able to view it.	I do think they should have the right because if it is to apprehend offenders then it can only be a positive. I think it should be specifically legislated so it is not misused.
		I feel that this right would be very beneficial to police personnel, to investigations and to the public's perception/confidence in the police. I believe this right would create opportunities to improve investigations, gather further evidence and intelligence and information sharing (and internationally) and could assist in obtaining more successful prosecutions for suspects. I feel having this right could also create opportunities to create further/new strategies and processes in keeping the public safe as it could open further avenues to police types of crime more effectively, that are currently difficult to do so due to not having this right so accessible. also, personally, I feel that having this right could create a greater sense of responsibility as a police officer, to the public, in positive way, to show that they are capable and worthy of having such a right.	100%. I think that private information is obtained by us whenever we enter someones house, search their pockets or investigate them. We could potentially and at any stage see or hear something totally private (and completely defaming or controversial) and we would be expected to handle this information sensitively and according to legislation. The PACE powers and Misuse of Drugs act powers (among others) which allow us to justify these kinds of searches are based on suspicion of criminality only. If we suspect someone of criminality - why are their private online and open source places much more difficult or impossible for us to investigate. It is beyond me. If we find evidence of criminality then we will investigate it.	Too bad if people committing offences don't like it. We are the police. If we find private info then we are expected to deal with it legally. If we fail to do that we should be prosecuted in turn. Who is it down to to lobby for and correct this? Just like a private company could not deny us access to their physical buildings if we could justify it - if these software giants want to operate in the UK and access the UK customers then they must have a method whereby their UK customer's law enforcement representation can safeguard and protect their population. If they don't want to allow us that - then ban them from the UK. Why does the government care? It's not like half of them pay the UK our due of tax is it. People aren't going to move overseas or not visit here because Snapchat gets banned. They just might if the use of social media and totally private, impenetrable communication systems gives terrorists and criminals an effective way to operate here.
Open source information - yes. Data that people place on social media which is public carries little or no expectation of privacy. Such data that carries with it restrictions placed by the user, e.g. restricted posts on social media, should require the usual RIPA justifications and powers in order to access.	Criminals are using the internet more and we as, a service, need to be able to freely use this in the fight and investigation of crime	if its for police work then it should be freely available, there should be no restrictions on what police can look at if its open source		

Figure 28. Qualitative Comments and Thematic Coding: Question 4.

Thematic Coding	Themes	Respondent Answers	Respondent Answers	Respondent Answers
What are the phenomena of concern being mentioned?	Q.4 Knowledge Section - The privacy/security debate is an important one for society and the legitimacy of the police. Do you think the police should automatically have the right to view open source information regardless of how personal, for policing purposes- [Comment]			
Why – Reasons provided or constructed?	Yes - Access should be automatic	Open source info is just that open to all.	If its a policing purpose then yes	It's open source. There's no expectation of privacy.
		The Police are an essential part of the fabric of society and should not be excluded from collecting this info.		
		It's not a matter of there being a right, if you make personal information available to anyone online you are allowing yourself to be viewed by any person. Any person with any grumbles can seek to improve their own online security.	Anything that is posted or stored in a public forum should be able to be viewed for policing purposes.	I feel that information that is posted into an online forum should be accessible by police, particularly if it would assist in the execution of their duty, whether this is to find a Misper or outstanding suspect.
		Open source but protected by privacy settings should be protected by DSA and Undercover policing authorities. Other than that post online for all to see and open profiles are visible to everyone including the public and so therefore police should be able to work on it.	Access to what is in the public domain is game on. Anything that is private is not. Threshold tests apply before accessing private data. From my limited knowledge balance appears to be correct as it stands.	If it is open for the public at large to view because of minimal security settings it should be fine for us.
		If someone does not have restrictive security on their account and anyone can view it then why not allow the police to use that. If the information is protected then that is a different matter.	We know about the recent success Terrorist organisations have had by using internet to spread their propaganda and recruit terrorist to carry out acts of terror. Why shouldn't police be allowed to use internet as a tool to fight back and combat the issues that are faced by the communities and nations?'	If it has been shared in the public domain and is available for all persons to see then I feel we should have a right to view it. The digital world is just as real now as the physical one. We just view it in a different way. We would not ignore information obtained in the physical world or stop seeking out evidence at the scene of a crime. So why should we act any differently online?
		In the world that I work we are constantly looking at the welfare of that person and trying to ensure safeguarding of them. Often, we have a feeling about something, which if we had access to one specific area of information it may either confirm or negate a risk to that person. We rarely have powers to demand information when someone is missing which is a challenge when trying to identify risk and negate it.	By definition open-source is publically available information. Police need to have the tools and the powers in order to conduct effective investigations and prosecutions. Many offences are now taking place in "cyber-space" so Police need to have the powers and ability to pursue those leads. As with most investigative tools, open source should be subject to uses for the purpose of prevention and detection of crime.	For serious crime I believe the protection of the public from crime over-rides the right to privacy on the internet particularly in terrorist and child protection cases. I know with enough evidence we can get a Courts permission to access personal sites but we need to monitor the level of risk taking place prior to obtaining the right level of evidence. I am not suggesting any officer can look where they like just that those investigating the most serious crimes can be authorised by a senior officer.
		If you have nothing to hide then you wont get in trouble	Any information which can be obtained through the same levels of access as a normal member of the public should be 'open'.	If it is in the open domain we should have the same right to access the information provided we are using overt methods to obtain it. To be blunt, if people are stupid enough to post information in an open forum that they don't want anyone to see, well what can you say!
		Privacy and private information are, by definition not open and therefore not public. RIPA governs this area.	Criminals should have no hiding places.	if it is freely available on the internet then everyone has the right to view it. the police should be no different, i think the public would expect that as a minimum
		In a threat to life incident, this should be the case.	Definitely ... a honest member of the public should have nothing to hide or be worried about...	If it is in open source then it is in public domain. The individual could easily protect accounts - as is commonly done - but if they chose not to, then anyone can see and access this public information.
		To assist locating and apprehending offenders and venerable members of public.	Criminals are hiding as know this to be the case	If it is open source it seems counter-intuitive not to be able to view it. If the information is willingly posted publicly be the subject then anyone should be able to view it.
		If the information is on an open source it is incumbent upon the data source themselves to manage their exposure online. Would a person stand in the street and shout the information that they share online? Unlikely. However, if they put it in an open forum online then I see no reason why the police should not be able to view that and act on it, no matter how personal the information is, provided that it is properly captured, assessed with all other intelligence or evidence and consistent in its provenance.	Due to current restrictions we are not able to view personal or direct messages only those available to the general public, by the time we have instructed users to capture this themselves the evidence can be deleted by the other party. If we were able to do this then more evidence could be secured, however measures would need to be in place to govern when this would be appropriate	If it is open source then the person in question has already permitted at some point for that information to be made public. If we could view something as a member of the public then why should that ever be inadmissible as evidence if viewing it from a policing point.
		This would save time, money and police resources.	Crime no matter how serious or not is crime. Clearly we need to use what we can.	If it is open source and available to any given member of the public then it would be very strange if the police couldn't use it. We need to be more careful when people are putting information out in a more restricted manner.
		The material is in the public and should be available for police purposes	Cut the red tape and let us crack on and lock up criminals. If I want to investigate my wife I can do that without MPS tools in my own tmie!	If it is open source then the information is already available, you are not intrusively entering 'private' information.
		some many cases could have been won,	Corruption is evident in all realms of society. All we need is easy access to information which any other member of the public can get anyway without any issues, passwords or authority.	If open source is left open and freely available (i.e not requiring a friend request, no privacy settings) then the police should be able to view it as any other member of the public or organisation in the world can.
		The information is in the public domain and available to anyone who searches for it. In the majority of cases the individual has posted information online freely knowing it will be accessible by anyone including law enforcement agencies.	By definition, open source information is accessible by anyone through the use of a computer.	If it's available to the public, why shouldn't the police be able to view it
		It is posted for all to see. Up to MoP to makeit private if wish to protect from police, press etc	If it's information that an individual has made freely available to the wider public I see no issue in police accessing and using it for investigative purposes. Anything which is beyond that should be accessed only once the proper authority has been granted and it's proportionate and justified etc	If it is on an open forum, then it should be allowed for officers to view too.
		It is a choice to use Social Media Platforms and it is clear that the more information you put onto digital accounts the more you leave a footprint. If you have no Facebook account it cannot be accessed.	Privacy is an ethical issue. Law enforcement agencies are required to investigate all lines of enquiry to either prove or disprove, by law	for the purposes of national security / solving crime, if you're a law abiding individual you will not be of interest to law enforcement
		it is open source. people have chosen to have their information open and freely available (be it through choice or poor practice) - it is in the public domain and therefore fair game.	We are safeguarding persons primarily intrusive checks help the intel process.	If it is open source, then it is no different to witnessing something in a public place.
		If you create an open, public profile, then we have as much right as anyone to view that profile (as long as it is for a policing purpose and is within RIPA guidelines around right to privacy, collateral intrusion, etc).	It has always been my view (and one upheld by a number of court judgements) that material made available on the internet that can be viewed publically has been published by the author.	Everyone has the option to choose their privacy settings on social media, so if someone has allowed their profile to be public, then this should not be viewed as a breach of privacy.
		its the same as walking down the street if its online there can be no expectation of privacy. Its public forum so owner has agreed for othes to see it	At the point, the information ceases to be 'private' and anyone, including the police, can access it.	For a suitably serious policing purpose then I think that any online information should be in play.
Its in the public domain so why not, if people what to hide this information then security and information security should be a personal responsibility	if you put information in the public domain then and you dont set your security settings to prevent anyone viewing info then its in the public domain	People post information voluntarily, police should have access to it		
Much of the information is open and not protected its not private you need a policing purpose to justify what you are doing	Privacy in a liberal democracy is important. It depends what you mean by open source ? If you mean something that anyone can see by a quick internet search then yes, its open source.	if you have nothing to hide what is there to worry about! If we had this access it may make people think twice about what they share on social media.		
We are accessing information that is already in the public domain. The public will be exasperated if we cannot access information that they themselves can because it's already in the public sphere.	If we are expected to 'police' and investigate, then we need proper access to any and all information. The level and depth of that info should then depend on the type of investigation, along the lines of standard applications e.g. proportionately, collateral intrusion etc.	People are made aware of whatever they put on social media or the internet is available to anybody including law enforcement agencies.		

Figure 28. Qualitative Comments and Thematic Coding: Question 4.

Thematic Coding	Themes	Respondent Answers	Respondent Answers	Respondent Answers
What are the phenomena of concern being mentioned?	Q.4 Knowledge Section - The privacy/security debate is an important one for society and the legitimacy of the police. Do you think the police should automatically have the right to view open source information regardless of how personal, for policing purposes- [Comment]			
Why – Reasons provided or constructed?	Yes - Access should be automatic	Open source info is just that open to all.	If its a policing purpose then yes	It's open source. There's no expectation of privacy.
		The Police are an essential part of the fabric of society and should not be excluded from collecting this info.		
		It's not a matter of there being a right, if you make personal information available to anyone online you are allowing yourself to be viewed by any person. Any person with any grumbles can seek to improve their own online security.	Anything that is posted or stored in a public forum should be able to be viewed for policing purposes.	I feel that information that is posted into an online forum should be accessible by police, particularly if it would assist in the execution of their duty, whether this is to find a Misper or outstanding suspect.
		Open source but protected by privacy settings should be protected by DSA and Undercover policing authorities. Other than that post online for all to see and open profiles are visible to everyone including the public and so therefore police should be able to work on it.	Access to what is in the public domain is game on. Anything that is private is not. Threshold tests apply before accessing private data. From my limited knowledge balance appears to be correct as it stands.	If it is open for the public at large to view because of minimal security settings it should be fine for us.
		If someone does not have restrictive security on their account and anyone can view it then why not allow the police to use that. If the information is protected then that is a different matter.	We know about the recent success Terrorist organisations have had by using internet to spread their propaganda and recruit terrorist to carry out acts of terror. Why shouldn't police be allowed to use internet as a tool to fight back and combat the issues that are faced by the communities and nations?'	If it has been shared in the public domain and is available for all persons to see then I feel we should have a right to view it. The digital world is just as real now as the physical one. We just view it in a different way. We would not ignore information obtained in the physical world or stop seeking out evidence at the scene of a crime. So why should we act any differently online?
		In the world that I work we are constantly looking at the welfare of that person and trying to ensure safeguarding of them. Often, we have a feeling about something, which if we had access to one specific area of information it may either confirm or negate a risk to that person. We rarely have powers to demand information when someone is missing which is a challenge when trying to identify risk and negate it.	By definition open-source is publically available information. Police need to have the tools and the powers in order to conduct effective investigations and prosecutions. Many offences are now taking place in "cyber-space" so Police need to have the powers and ability to pursue those leads. As with most investigative tools, open source should be subject to uses for the purpose of prevention and detection of crime.	For serious crime I believe the protection of the public from crime over-rides the right to privacy on the internet particularly in terrorist and child protection cases. I know with enough evidence we can get a Courts permission to access personal sites but we need to monitor the level of risk taking place prior to obtaining the right level of evidence. I am not suggesting any officer can look where they like just that those investigating the most serious crimes can be authorised by a senior officer.
		If you have nothing to hide then you wont get in trouble	Any information which can be obtained through the same levels of access as a normal member of the public should be 'open'.	If it is in the open domain we should have the same right to access the information provided we are using overt methods to obtain it. To be blunt, if people are stupid enough to post information in an open forum that they don't want anyone to see, well what can you say!
		Privacy and private information are, by definition not open and therefore not public. RIPA governs this area.	Criminals should have no hiding places.	if it is freely available on the internet then everyone has the right to view it. the police should be no different, i think the public would expect that as a minimum
		In a threat to life incident, this should be the case.	Definitely ... a honest member of the public should have nothing to hide or be worried about...	If it is in open source then it is in public domain. The individual could easily protect accounts - as is commonly done - but if they chose not to, then anyone can see and access this public information.
		To assist locating and apprehending offenders and venerable members of public.	Criminals are hiding as know this to be the case	If it is open source it seems counter-intuitive not to be able to view it. If the information is willingly posted publicly be the subject then anyone should be able to view it.
		If the information is on an open source it is incumbent upon the data source themselves to manage their exposure online. Would a person stand in the street and shout the information that they share online? Unlikely. However, if they put it in an open forum online then I see no reason why the police should not be able to view that and act on it, no matter how personal the information is, provided that it is properly captured, assessed with all other intelligence or evidence and consistent in its provenance.	Due to current restrictions we are not able to view personal or direct messages only those available to the general public, by the time we have instructed users to capture this themselves the evidence can be deleted by the other party. If we were able to do this then more evidence could be secured, however measures would need to be in place to govern when this would be appropriate	If it is open source then the person in question has already permitted at some point for that information to be made public. If we could view something as a member of the public then why should that ever be inadmissible as evidence if viewing it from a policing point.
		This would save time, money and police resources.	Crime no matter how serious or not is crime. Clearly we need to use what we can.	If it is open source and available to any given member of the public then it would be very strange if the police couldn't use it. We need to be more careful when people are putting information out in a more restricted manner.
		The material is in the public and should be available for police purposes	Cut the red tape and let us crack on and lock up criminals. If I want to investigate my wife I can do that without MPS tools in my own tmie!	If it is open source then the information is already available, you are not intrusively entering 'private' information.
		some many cases could have been won,	Corruption is evident in all realms of society. All we need is easy access to information which any other member of the public can get anyway without any issues, passwords or authority.	If open source is left open and freely available (i.e not requiring a friend request, no privacy settings) then the police should be able to view it as any other member of the public or organisation in the world can.
		The information is in the public domain and available to anyone who searches for it. In the majority of cases the individual has posted information online freely knowing it will be accessible by anyone including law enforcement agencies.	By definition, open source information is accessible by anyone through the use of a computer.	If it's available to the public, why shouldn't the police be able to view it
		It is posted for all to see. Up to MoP to makeit private if wish to protect from police, press etc	If it's information that an individual has made freely available to the wider public I see no issue in police accessing and using it for investigative purposes. Anything which is beyond that should be accessed only once the proper authority has been granted and it's proportionate and justified etc	If it is on an open forum, then it should be allowed for officers to view too.
		It is a choice to use Social Media Platforms and it is clear that the more information you put onto digital accounts the more you leave a footprint. If you have no Facebook account it cannot be accessed.	Privacy is an ethical issue. Law enforcement agencies are required to investigate all lines of enquiry to either prove or disprove, by law	for the purposes of national security / solving crime, if you're a law abiding individual you will not be of interest to law enforcement
		it is open source. people have chosen to have their information open and freely available (be it through choice or poor practice) - it is in the public domain and therefore fair game.	We are safeguarding persons primarily intrusive checks help the intel process.	If it is open source, then it is no different to witnessing something in a public place.
		If you create an open, public profile, then we have as much right as anyone to view that profile (as long as it is for a policing purpose and is within RIPA guidelines around right to privacy, collateral intrusion, etc).	It has always been my view (and one upheld by a number of court judgements) that material made available on the internet that can be viewed publically has been published by the author.	Everyone has the option to choose their privacy settings on social media, so if someone has allowed their profile to be public, then this should not be viewed as a breach of privacy.
		its the same as walking down the street if its online there can be no expectation of privacy. Its public forum so owner has agreed for othes to see it	At the point, the information ceases to be 'private' and anyone, including the police, can access it.	For a suitably serious policing purpose then I think that any online information should be in play.
Its in the public domain so why not, if people what to hide this information then security and information security should be a personal responsibility	if you put information in the public domain then and you dont set your security settings to prevent anyone viewing info then its in the public domain	People post information voluntarily, police should have access to it		
Much of the information is open and not protected its not private you need a policing purpose to justify what you are doing	Privacy in a liberal democracy is important. It depends what you mean by open source ? If you mean something that anyone can see by a quick internet search then yes, its open source.	if you have nothing to hide what is there to worry about! If we had this access it may make people think twice about what they share on social media.		
We are accessing information that is already in the public domain. The public will be exasperated if we cannot access information that they themselves can because it's already in the public sphere.	If we are expected to 'police' and investigate, then we need proper access to any and all information. The level and depth of that info should then depend on the type of investigation, along the lines of standard applications e.g. proportionately, collateral intrusion etc.	People are made aware of whatever they put on social media or the internet is available to anybody including law enforcement agencies.		

Figure 28. Qualitative Comments and Thematic Coding: Question 4.

Thematic Coding	Themes	Respondent Answers	Respondent Answers	Respondent Answers
What are the phenomena of concern being mentioned?	Q.4 Knowledge Section - The privacy/security debate is an important one for society and the legitimacy of the police. Do you think the police should automatically have the right to view open source information regardless of how personal, for policing purposes- [Comment]			
Why – Reasons provided or constructed?	Yes - Access should be automatic	Open source info is just that open to all.	If its a policing purpose then yes	It's open source. There's no expectation of privacy.
		The Police are an essential part of the fabric of society and should not be excluded from collecting this info.		
		It's not a matter of there being a right, if you make personal information available to anyone online you are allowing yourself to be viewed by any person. Any person with any grumbles can seek to improve their own online security.	Anything that is posted or stored in a public forum should be able to be viewed for policing purposes.	I feel that information that is posted into an online forum should be accessible by police, particularly if it would assist in the execution of their duty, whether this is to find a Misper or outstanding suspect.
		Open source but protected by privacy settings should be protected by DSA and Undercover policing authorities. Other than that post online for all to see and open profiles are visible to everyone including the public and so therefore police should be able to work on it.	Access to what is in the public domain is game on. Anything that is private is not. Threshold tests apply before accessing private data. From my limited knowledge balance appears to be correct as it stands.	If it is open for the public at large to view because of minimal security settings it should be fine for us.
		If someone does not have restrictive security on their account and anyone can view it then why not allow the police to use that. If the information is protected then that is a different matter.	We know about the recent success Terrorist organisations have had by using internet to spread their propaganda and recruit terrorist to carry out acts of terror. Why shouldn't police be allowed to use internet as a tool to fight back and combat the issues that are faced by the communities and nations?'	If it has been shared in the public domain and is available for all persons to see then I feel we should have a right to view it. The digital world is just as real now as the physical one. We just view it in a different way. We would not ignore information obtained in the physical world or stop seeking out evidence at the scene of a crime. So why should we act any differently online?
		In the world that I work we are constantly looking at the welfare of that person and trying to ensure safeguarding of them. Often, we have a feeling about something, which if we had access to one specific area of information it may either confirm or negate a risk to that person. We rarely have powers to demand information when someone is missing which is a challenge when trying to identify risk and negate it.	By definition open-source is publically available information. Police need to have the tools and the powers in order to conduct effective investigations and prosecutions. Many offences are now taking place in "cyber-space" so Police need to have the powers and ability to pursue those leads. As with most investigative tools, open source should be subject to uses for the purpose of prevention and detection of crime.	For serious crime I believe the protection of the public from crime over-rides the right to privacy on the internet particularly in terrorist and child protection cases. I know with enough evidence we can get a Courts permission to access personal sites but we need to monitor the level of risk taking place prior to obtaining the right level of evidence. I am not suggesting any officer can look where they like just that those investigating the most serious crimes can be authorised by a senior officer.
		If you have nothing to hide then you wont get in trouble	Any information which can be obtained through the same levels of access as a normal member of the public should be 'open'.	If it is in the open domain we should have the same right to access the information provided we are using overt methods to obtain it. To be blunt, if people are stupid enough to post information in an open forum that they don't want anyone to see, well what can you say!
		Privacy and private information are, by definition not open and therefore not public. RIPA governs this area.	Criminals should have no hiding places.	if it is freely available on the internet then everyone has the right to view it. the police should be no different, i think the public would expect that as a minimum
		In a threat to life incident, this should be the case.	Definitely ... a honest member of the public should have nothing to hide or be worried about...	If it is in open source then it is in public domain. The individual could easily protect accounts - as is commonly done - but if they chose not to, then anyone can see and access this public information.
		To assist locating and apprehending offenders and venerable members of public.	Criminals are hiding as know this to be the case	If it is open source it seems counter-intuitive not to be able to view it. If the information is willingly posted publicly be the subject then anyone should be able to view it.
		If the information is on an open source it is incumbent upon the data source themselves to manage their exposure online. Would a person stand in the street and shout the information that they share online? Unlikely. However, if they put it in an open forum online then I see no reason why the police should not be able to view that and act on it, no matter how personal the information is, provided that it is properly captured, assessed with all other intelligence or evidence and consistent in its provenance.	Due to current restrictions we are not able to view personal or direct messages only those available to the general public, by the time we have instructed users to capture this themselves the evidence can be deleted by the other party. If we were able to do this then more evidence could be secured, however measures would need to be in place to govern when this would be appropriate	If it is open source then the person in question has already permitted at some point for that information to be made public. If we could view something as a member of the public then why should that ever be inadmissible as evidence if viewing it from a policing point.
		This would save time, money and police resources.	Crime no matter how serious or not is crime. Clearly we need to use what we can.	If it is open source and available to any given member of the public then it would be very strange if the police couldn't use it. We need to be more careful when people are putting information out in a more restricted manner.
		The material is in the public and should be available for police purposes	Cut the red tape and let us crack on and lock up criminals. If I want to investigate my wife I can do that without MPS tools in my own tmie!	If it is open source then the information is already available, you are not intrusively entering 'private' information.
		some many cases could have been won,	Corruption is evident in all realms of society. All we need is easy access to information which any other member of the public can get anyway without any issues, passwords or authority.	If open source is left open and freely available (i.e not requiring a friend request, no privacy settings) then the police should be able to view it as any other member of the public or organisation in the world can.
		The information is in the public domain and available to anyone who searches for it. In the majority of cases the individual has posted information online freely knowing it will be accessible by anyone including law enforcement agencies.	By definition, open source information is accessible by anyone through the use of a computer.	If it's available to the public, why shouldn't the police be able to view it
		It is posted for all to see. Up to MoP to makeit private if wish to protect from police, press etc	If it's information that an individual has made freely available to the wider public I see no issue in police accessing and using it for investigative purposes. Anything which is beyond that should be accessed only once the proper authority has been granted and it's proportionate and justified etc	If it is on an open forum, then it should be allowed for officers to view too.
		It is a choice to use Social Media Platforms and it is clear that the more information you put onto digital accounts the more you leave a footprint. If you have no Facebook account it cannot be accessed.	Privacy is an ethical issue. Law enforcement agencies are required to investigate all lines of enquiry to either prove or disprove, by law	for the purposes of national security / solving crime, if you're a law abiding individual you will not be of interest to law enforcement
		it is open source. people have chosen to have their information open and freely available (be it through choice or poor practice) - it is in the public domain and therefore fair game.	We are safeguarding persons primarily intrusive checks help the intel process.	If it is open source, then it is no different to witnessing something in a public place.
		If you create an open, public profile, then we have as much right as anyone to view that profile (as long as it is for a policing purpose and is within RIPA guidelines around right to privacy, collateral intrusion, etc).	It has always been my view (and one upheld by a number of court judgements) that material made available on the internet that can be viewed publically has been published by the author.	Everyone has the option to choose their privacy settings on social media, so if someone has allowed their profile to be public, then this should not be viewed as a breach of privacy.
		its the same as walking down the street if its online there can be no expectation of privacy. Its public forum so owner has agreed for othes to see it	At the point, the information ceases to be 'private' and anyone, including the police, can access it.	For a suitably serious policing purpose then I think that any online information should be in play.
Its in the public domain so why not, if people what to hide this information then security and information security should be a personal responsibility	if you put information in the public domain then and you dont set your security settings to prevent anyone viewing info then its in the public domain	People post information voluntarily, police should have access to it		
Much of the information is open and not protected its not private you need a policing purpose to justify what you are doing	Privacy in a liberal democracy is important. It depends what you mean by open source ? If you mean something that anyone can see by a quick internet search then yes, its open source.	if you have nothing to hide what is there to worry about! If we had this access it may make people think twice about what they share on social media.		
We are accessing information that is already in the public domain. The public will be exasperated if we cannot access information that they themselves can because it's already in the public sphere.	If we are expected to 'police' and investigate, then we need proper access to any and all information. The level and depth of that info should then depend on the type of investigation, along the lines of standard applications e.g. proportionately, collateral intrusion etc.	People are made aware of whatever they put on social media or the internet is available to anybody including law enforcement agencies.		

Figure 28. Qualitative Comments and Thematic Coding: Question 4.

Thematic Coding	Themes	Respondent Answers	Respondent Answers	Respondent Answers
What are the phenomena of concern being mentioned?	Q.4 Knowledge Section - The privacy/security debate is an important one for society and the legitimacy of the police. Do you think the police should automatically have the right to view open source information regardless of how personal, for policing purposes- [Comment]			
Why – Reasons provided or constructed?	Yes - Access should be automatic	Also if information is not protected/secure it is available for the public or anyone else to view.	It is the choice the poster has made to publish this into an open forum, no different, for example, from leaving a poster on a lamp-post.	If you make an application to join a social media group, your contract states " we will share information with law enforcement agencies", its clear an unambiguous from the start, if you access social media, put items there, DONT MOAN about the police finding it.
		Its in the public domain. each person has the freedom to choose what is and is not placed in the public domain by them.	It's in the public domain	Public Domain. Prevention and detection of crime?!
		If its placed in any sort of open forum, I.E. online, Facebook, Twitter then the Police should be able to use this	If the individual has declined to set their profile to private it is the equivalent of painting the message in 6 foot letters on a billboard, anyone can and will see it.	If journalists and the public can look at it/use it (for example an open Facebook account), we look incompetent as an organisation if we don't at least try and exploit it for legitimate policing purposes. We are YEARS out of date.
		If it is something that is in the public domain which the Police have not had to uncover through engaging with the person then I do not think it is unethical or unlawful if it is publically available then it is fair game. Transposing this argument to traditional policing, officers would have to wear blinkers in the street, were this the case!	If the information is available to the public, police are entitled to see it. I am not aware of it being used for another reason so I can't provide a circumstance other than the ones in which I use it which as you can see is very basic.	If members of the public are leaving their social media accounts open then yes - just as if they were putting posters up in their windows at home or commenting verbally in public. However if the profiles are closed then just as when your front door to your house is closed only when a warrant is obtained can police enter, I think the police should have to go before a court and then onto the companies who run these sites prior to having access.
		If information is shared by a 3rd party, whether it be a social media profile, or by using google... the information is out there and can be accessed. The only important factor needs to be the grading of its reliability	If information is freely available it should be useable. It can get embarrassing if we are unable to access information which members of the public can	If information is posted online on unrestricted accounts then Polcie are in their rights to view and makes use of this information, however if a person protects their account and the information isn't readily available to the general public authority should be gained before accessing and using this information
		If information is available in an open forum then of course police should be allowed to have access to it. If there is a valid policing reason then all information should be made available, especially if it may hinder an investigation.	If information is in the public domain, the user must accept that any agency could look at it in the same way any member of the public could. There are plenty of ways to secure information if desired.	If it could assist in finding a missing person for instance then this would be very useful
		If it is available open source without the use of passwords and hacking then it is fair game for police. The issues in NOT doing it is that victims will do it on our behalf which when trying to clear up and present as evidence is always a trying process. If police do it themselves the product will be cleaner and readily convertible into evidence (Statement or exhibit).	If it available on the wider internet it seems obvious that the police should also have access to it.	If it falls within your given definition of 'Open Source' (namely that it's visible to us as it is to any member of the public) then yes, it's available to be seen and should be utilised. If someone's 'however personal' information has been put in the public domain by them, then I fail to see how they could complain if we made use of it.
		Yes, to assist with investigations where there is a risk to a person's safety and the information could assist in finding them/helping them		

Figure 28. Qualitative Comments and Thematic Coding: Question 4.

Thematic Coding	Themes	Respondent Answers	Respondent Answers	Respondent Answers
What are the phenomena of concern being mentioned?	Q.4 Knowledge Section - The privacy/security debate is an important one for society and the legitimacy of the police. Do you think the police should automatically have the right to view open source information regardless of how personal, for policing purposes- [Comment]			
Why – Reasons provided or constructed?	No - Access should not be automatic	I disagree that Police should be able to routinely access everyone's information without a crime even being suspected of being committed.*	No, because an individual still has the basic human right to privacy, so it should only be used where it can be fully justified	I don't think this is the case to look for information at hoc basis but always good to be justifiable.
		whilst I don't agree that we should have automatic access, the process is too far the other way, and if it is relevant can be made quicker with a reduction in the number of people each application needs to go through to be agreed.	Not all police officers are trustworthy, so a higher rank such as a Superintendent should have the final say - needs control for the purpose of protecting police	basic human and social rights should be protected and respected to save the fabric of the society
		Without some control over what we view, we are likely to lose an ability to do so in the future.	HRA	I don't think that it should be automatic, I think there needs to be regulated access to a persons private information, but there shouldn't be any clause to inhibit police research due to the sensitivity of the information.
		Unless it is for criminal matter then they should not be allowed as some might abuse this power	It would be misused	We should have to justify the use but it should be a case of adding a report reference and the officer conducting the research just checks the CRIS. Its time consuming having to do a form for each application
		There has to be a respect for privacy and a legitimacy for the application for the information.	everybody has a right to data protection. That kind of information should be requested separately if access is needed	It should not be a given that Police have access to persons information. HOWEVER, should the investigation be of a certain significance or could minimise the risk to another person, then (with the correct authority) we should have at least the opportunity to look at such information.
		there are some that would use it in the wrong way and abuse the fact that it is automatically our right to view open source information therefore ruining it for everyone else	I think it needs to be carefully regulated. it is an endless resource unlike other systems like PNC and CRIMINT so it needs to be properly monitored and restricted where necessary.	Its a good argument for both sides. I tend to lean towards that we should not automatically have rights as our policing is already under scrutiny by the public and they believe a certain amount of privacy is important to keep. It's a bit like "Big Brother is watching you".
		The police need to be mindful of privacy and freedom of expression in all aspects of policing.	It would be open to abuse but if someone has put their details on social media for all to see.....	People still have a right to privacy therefore it is correct that police access to personal information is restricted
		There are rules and SOPs in place to prevent the misuse of material, but there is very much a need for access to this material. Disclosure rules MUST be followed but access to all material is needed, given the reliance society has now on the internet / social media and not having access may harm an investigation that will either assist prove an allegation or identify evidence that disproves the allegation.	We all have a right to a private life, unrestricted access may open ethical dilemmas. As a police officer I already resent the amount of control "the Job" has over my life, I really do not want "the state" to be able to freely fish around in my personal matters. If you look hard enough in anyones life you will find something the person will not want to be judged by others on.	No not an automatic right (this would be massively open to allegations of abuse) but should be much easier than it is. Public assume we have vastly easier and greater access than we do, which can make managing their expectations a challenge.
		Being able to view public accounts for certain policing purposes could be beneficial - eg. To help trace a high risk missing person or to help trace wanted offenders. Police should NOT be accessing public profiles to just monitor previous offenders for developing intelligence otherwise this could be viewed as intrusive - just because somebody has committed a crime once, does not mean they will commit another.	When it comes to more serious offences, I think the question is less whether we should have the automatic right to view private, online information but whether the public would expect us to be able to if it was necessary, proportionate and for a policing purpose. I think they would, and I think if we want to be effective in combating crime we need to have a more effective online presence. Programming and coding issues aside, it seems ridiculous to me - for example - that we can't read anything on an iPhone 6 without a pin. I know this is not a policing debate per se, but it is illustrative of our impotence in the face of crime conducted on smart phones and online. We lose countless PWITS cases every single week because no-one can look at the phone so we give up and charge for possession. Perhaps it is an issue of education (or rather ignorance on borough), but I have very little faith in our abilities to exploit technology where it is important to an investigation.	We should follow the same rules for the real world - IE use of RIPA. The public should have some expectation of privacy when security settings are applied. If social media is being used as a tool to find out information relating to individuals policing should adhere to the principles of proportionality and collateral intrusion. That said we should not be tied down with bureaucracy when conducting initial fact finding enquires. However when directed at individuals RIPA should be followed to protect the public and MPS staff by having accountability with external oversight. (OSC inspections)
		The same we cannot obtain a persons medical history, banking details, their personal information online should be allowed a degree of privacy. As with the other areas of privacy, it can be overridden when it is proportionate, necessary, legal and accountable.	However, if you mean something that requires a password or security setting to be bypassed then no. To have such access, without oversight, would be no different from police opening someone's post. I believe it would undermine the trust in police."	Collateral intrusion can only happen for the right reasons. There always be an idiot that wants to check up on his or her ex partner's social media account.
		Some people are innocent parties in criminal activity, and sometimes are unaware as to what is going on. Their private lives should not be intruded upon because of someone else's indiscretion. Privacy should remain private.	Users of social media have an expectation of privacy, covert intrusion into this can cause reputational damage. The legal framework is however somewhat sketchy and requires updating to take into account expectations and necessity of intrusion.	Automatically is the word that I disagree with, there must be a specific reason, not fishing.
		Risk to obtaining too much private information from collateral contacts - Breaches Article 8	Police should not have access to anyone's personal information unless there is a legitimate reason for them to have access to it.	Police officer if you cannot be trusted.
		Its our job to protect the public, the civil liberty groups need to stop obstructing us upholding the law.	Some level of protection needs to be in place to ensure that the information is requested in a	I believe there is an argument that if it is openly accessible then an individual is exposing themselves to the risk that others may use this information or at least monitor it. If a profile is set to private and you have to request access and you do so under a false name (not police related) then I think this needs more stringent guidance and supervision.
People are entitled to an expectation of privacy online just as they are on the street. We cannot just go and search someone on the street so we should not be able to search online without reasonable grounds.	It depends. I don't think it should be readily available accessible to police as there may be abuse of the system. Any breach of privacy must be justified.			

Figure 28. Qualitative Comments and Thematic Coding: Question 4.

Thematic Coding	Themes	Respondent Answers	Respondent Answers	Respondent Answers
What are the phenomena of concern being mentioned?	Q.4 Knowledge Section - The privacy/security debate is an important one for society and the legitimacy of the police. Do you think the police should automatically have the right to view open source information regardless of how personal, for policing purposes- (Comment)			
Why – reasons provided or constructed?	Balance between privacy and security	IF IT IS JUSTIFIED FOR POLICING PURPOSES FOR INDICTABLE OFFENCE	If it is for the purpose of policing, I agree.	I think if they can justify why it was viewed then I see no problem
		Policed properly and kept safe then there is no reason why we cannot access it for a Policing Purpose.	I agree with online UC investigators having authority for communications etc, but at my level repeated viewing should for things in the public domain should not be under RIPA. expectation that anything online is public.	as long as its on a social media account for all to see then yes
		yes, though depends on the nature of the offence. If it is one of national security, life endangerment etc then yes as the seriousness of the investigation should take precedence over criminal activity/privacy.	Grey area, requires maturity by OIC and oversight. Yes when dealing with credible to an individual, more grey when dealing with monitoring of live feed from a public protest.	As long as it is dealt with and disposed of correctly if not required. There is no point being a
		Yes but with conditions - must be for a legitimate and legal reason	If its in relation to helping solve a crime or finding a missing or vulnerable person or child then yes, Police should have access to a plethora of information	As long as it's for policing purposes I do not see any issues. If a person is innocent they would have nothing they need to hide and would have nothing to worry about. If the person is guilty... well law shouldn't protect the guilty...
		Only if its related to the job in question	If it's open source -it's open (if that is proportionate to the investigation)	As long as it is for a policing purpose and it is reasonable, then I think it should be lawful.
		We should always justify and account for viewing/obtaining personal information but in general if it is relevant to a Police investigation then the Police should have the right to view it.	If should still be governed by the seriousness of offence and reasons why this cannot be obtained through less intrusive means to maintain public confidence whilst I am a believer in nothing to hide why would you bother a lot of people see the right to privacy as a more serious matter and that I believe is the general consensus so safeguards must be kept in place.	AS LONG AS IT'S DONE FOR OFFICIAL REASONS I DON'T SEE A PROBLEM
		It's about being proportionate and how the service is perceived.	If the material is there for anyone to view without having to engage with the individual then they are fair game. In relation to private/closed accounts, then rightly, RIPA needs to be adhered to re, proportionality/necessity.	As long as it is for a valid policing purpose and can be shown to be PLAN and does not infringe any current legislation, i.e. legal privilege, etc.
		We should always have to provide a sound reason: just 'cause a large section of society now chose to effectively undress by an open window (to use a faintly off-beat metaphor) doesn't mean we should all stand by window and stare on the off chance of catching a glimpse of someone's underwear. However, that does not mean that everything should go down the RIPA route as, to continue with the earlier metaphor, if you're daft enough not to close your curtains then you should be aware that there's a chance someone will see you in a state of undress.	Intrusion should always be necessary and proportional to the objectives and within the law.	As long as it is not abused. If it is to locate an offender or find someone at risk then we should have the right to do so.
		Yes, certainly if the case is 'serious' or the investigation involves 'saving life or limb'.	In certain very specific circumstances there should be a justification but this should be limited to only the most serious investigations in which an ongoing threat to life exists i.e. terrorism investigations.	As with all things we should be held accountable.
		There must be a justifiable level of intrusion.	Yes, but to a degree and within reason for specific crimes. Otherwise this would leave officers open to criticism..	As with anything, if it can be justified & is reasonable & proportionate
		We are only looking at this information as part of an investigation. As long as the officer can justify looking at the information in this day of age we should be able to look at it without loads of paperwork. This is all information which is available to the public anyway.	Clearly, any material that is only open to a closed group or section of the public is placed there in the expectation that it can only be viewed by those people. Any police access to that, and should be, carefully controlled to ensure that it is proportionate, legal, necessary and whomever accesses it can be held accountable for that access. That doesn't mean it should be difficult, just that there needs to be a process to consider these"	As long as there is a necessity and a legitimate policing purpose for it. Eg: Investigating indecent images, investigating sexual predators to establish their offending patterns and gather evidence against them, to intercept the communications especially when investigating
		If police can justify (ie threat to life/prevent crime) then fine"	Yes, as long as sufficiently justified and with the relevant authorities.	But I think the whole process needs to be simplified and made more accessible to all investigators who can justify accessing the open source information to assist them with their enquiries including lower level crimes.
		This is incredibly intrusive and shouldn't be used without justification	There should be a legitimate reason to use this, however if there is a genuine need then we should not have barriers which prevent us from thoroughly investigating an incident.	But it would have to be strictly monitored, to make sure that it was being viewed for a policing purpose and that it was relevant to the reason for looking at it in the first place but it must be justified and handled with discretion.
		There always has to be a legitimate reason for looking at personal/private information - there has to be safeguards in place. I do not think we should just have blanket authority to look at anyone's private information.	Yes, as long as it is accessible without overcoming or breaching user privacy settings. As long as we are seeing what has been made available for anyone to see.	But I think if you can prove the information is needed and can justify it, and have a log of who has authorised it for proper use, so that the system is not misused then I think access to that personnel information should be granted
		This is an argument around the world, people do have a right to privacy, why should it be any different to social media access? It would help to have access to it to assist investigations. there should be an access form for Social media where people consent (there is one for phones).	It has to be justified.	All viewing should be in accordance with PLAN not carte blanche.
		some accountability and rationale for accessing private information should remain	Where appropriate, using an approved framework, the use of open source information for modern police work is essential. However the way open source is used must be qualified / managed in line with intelligence/evidence guidelines.	Any research for potentially private information should address the proportionality and necessity. Failure may undermine the trust from the members of public and lead to an abuse.
		Not automatically. Depends on the seriousness of circumstances.	It is through processing, evaluation and proper assessment through an approved framework and guidelines best outcomes will result."	Absolutely, for a legitimate purpose
		Society is one that is now media based and will only become more prevalent within crime. If it is for policing purposes, then yes we should have access. Otherwise how can we do our job to its maximum capacity.	Yes with regards to Terrorism and cyber criminal investigation, but general use to spy on people I would say No. It all depends on the situation and what damage could be caused.	All and any access should be documented and a rational (brief) provided.
		PLAN method.	The internet, particularly social media and other sources of 'news' information, are vital for free speech/debate. The fact that the police can view this.	Apply code of ethics and no problem, up to person posting information what level of security they apply
		Should have a policing purpose, any realise to help an investigation or locate a wanted/missing person	Justification is key	A long as this can be justified
Police should have the right to view all information as long as the person can fully justify the reasons. Too many rules tie officers hands. If you are innocent then nothing to fear.	Subject to the proportionality of the enquiry - open source material is in the public domain - as a member of the public there would be no restriction on my ability to make open source enquiries - why should there be restrictions imposed when as a professional I would be making the enquiries to prevent / detect crimes of a serious nature.	If the data is being viewed for a policing purpose and is in relation to an investigation then it should be able to be used to protect/prevent harm or offences being caused to other members of public. If information obtained through open source research is considered private/personal, then the responsibility of the information not being widely accessible should lie with the individual who has made the information available through open source media.		
No, but they should have access with appropriate justification.	It would depend on the reason and explaining the reasons. Also how people's accounts are set up and what privacy settings they have in place and therefore what access they allow the general public to have to their life.	But only if it is proportionate (seriousness of the offence and risks to the victim)		
Police need to justify their actions with regards to the privacy of what we should do. We have found previously that police take advantage of their powers and so to make officers justify what they do is important	In line with the justifications for a RIPA authority i.e. prevention/decision of crime, national security, economic loss etc	As long as there is a legitimate purpose and not a fishing exercise to gather intel.		

Figure 28. Qualitative Comments and Thematic Coding: Question 4.

Thematic Coding	Themes	Respondent Answers	Respondent Answers	Respondent Answers
What are the phenomena of concern being mentioned?	Q.4 Knowledge Section - The privacy/security debate is an important one for society and the legitimacy of the police. Do you think the police should automatically have the right to view open source information regardless of how personal, for policing purposes- (Comment)			
Why – Reasons provided or constructed?	Balance between privacy and security	It would depend on the case	Subject to the proportionality of the enquiry - open source material is in the public domain - as a member of the public there would be no restriction on my ability to make open source enquiries - why should there be restrictions imposed when as a professional I would be making the enquiries to prevent / detect crimes of a serious nature.	This is because not all open source information is accurate. It is often inaccurate, subjective and can be malicious.
		Police need to adhere to legislation. You would not be able to watch somebody's house and see who is going in and out without directed surveillance authority - so you shouldn't be able to do repeated monitoring without correct permissions. If its P, L, A and N then should be no problem getting authority.	The extent of how much material is viewed should be tested as to how proportionate the research/investigation when taking into consideration the seriousness of the crime being committed.	As long as the individual can justify why they need the search of information I don't see a problem with it
		Organised crime and Counter Terrorism purposes or high risk misper yes otherwise no.	No only for investigative purposes investigating crime, dealing missing persons, high risk incidents and in some cases intelligence gathering.	if it assists a Police investigation than yes.
		must be reasonable and comply with the Human Rights Act	As with other covert tactics, the use of the covert internet research/engagement must be appropriately authorised and any work must be shown to be proportionate, lawful, accountable, necessary and ethical.	As long as submissions are accountable and proportionate then yes.
		Must be proportionate to offending / criminality	No, has to be justified in each case	Provided their is a legitimate reason for doing so, and not just researching for the sake of it.
		PLAN should always be at the forefront of an officers mind, even taking PLAN out of the equation the sheer quantity of information available means the police have to be targeted around how they use / access information.	When justified yes, definitely	It must be justified in order maintain balance of security with freedom and right to privacy
		only view if necessary for a policing purpose- why would you need to view for personal use?	Yes, if it is justifiable, relevant, proportionate and for a policing purpose we should be able to access it.	provided it can be justified. Is part of a genuine investigation and doesn't become a 'fishing' tool.
		It must form part of an investigation and grounds must exist for requesting it.	Providing that it is for legitimate purpose and with correct authority, I feel that it is an essential tool to locate Missing Persons and conduct research for investigative purposes	Providing the Necessity/Collateral Intrusion/Proportionality and Timeliness requirements are adhered to
		Only to the extent of targeted specific investigations, not simply to "police" social media. In the current circumstances it is far too easy for criminals to hide behind the internet.	Yes, for policing purposes but not as a fishing exercise legitimate need must exist.	it is proportionate to the investigation and assists, then def necessary
		But we would need to justify the use for legitimate purposes only such as Risk individuals being W/M or missing	In the prevention and detection of crime it should not be a hindrance.	Whilst there are those with false /corrupt intent as a Police Officer I am only ever looking at information with a legitimate Policing Purpose and we are doing it with one hand tied behind our backs standing on our heads using antiquated systems / techniques / processes
		But only where there is a legitimate risk to the wellbeing of the country as a whole or significant identifiable risk to an individual or group of individuals.	Like everything this will need to be justified. There are different levels of intrusion which will need to be taken into account. EG if someone does not have any restrictions on their account and we are looking at what any member of the public would have access to do not see any issues with this.	if it is justifiable, like call data etc then yes. At what level of justification / authorisation would depend on the information. The current system is very good, however more officers need to be trained and more covert terminals need to be made available without the awful hoop jumping to get them.
		If it will assist in an investigation and help bring suspects to justice. But should be monitored to make sure officers are not abusing the use of it though.	if for legitimate policing purposes yes.	If done for a policing purpose, it is necessary for the prevention/detection of crime and apprehension of offenders.
		If it's for policing purposes there is a legitimate reason behind it. It could lead to the prevention of a crime or the apprehension of a suspect. The safety of the public, which depending on the circumstances could mean one person or hundreds, should always be the priority.	I think there should still be a higher ranking officer to authorise such a search. I do think that the procedure for doing so should be simplified and made easier to use rather than what it is at present which is designed to discourage the search in the first place. If the search is very important the only achievement of the procedure is to delay and hinder.	The balance between respecting personal/private/sensitive data and the need to investigate crime, prevent damage to property, and preserve life will always need to be weighed up and considered. I imagine each case/investigation is judged on it's own merits, and what is to be gained from the information versus the intrusive nature of the investigation/research.
		If it relates to a serious offence then yes i think having immediate access would help. Again not to be abused by police forces.	I think the police should justify to an extent why they need that information. It should be generally given to us, but people should not be able to abuse it.	Whilst it should be more widely available to officers, police should be able to view / conduct internet research, but only if there is a legitimate policing purpose
		I believe there should be a ranking system in relation to the severity of the crime in terms of gaining access to open source info. However, in saying that, if that information is already freely available to the public then it is free game.	I think that whilst RIPA is not fit for the current purpose, I believe our interpretation of it in the OS context is actually not a bad system. I believe that most people are well aware of how their public facing data is handled. If you put something in the public domain, the majority understand that it can be seen by anyone, including the authorities. Its much the same as if you sat on a bus with a relative discussing the details of what you did last night in the presence and hearing of others, you'd expect that they can probably hear you and should tailor what you say appropriately. Equally, if you sat on that bus and was saying inappropriate things and an officer heard you, the public would expect the officer to act, much the same as if an officer online finds videos of violence or	I think that as long as HRA principles are followed there should be no problem with this. I'm not happy with the work 'automatically' in the question, as this implies no checks/balances should be followed, but following and considering HRA principles should alleviate this.
		I believe we should have to have grounds to view the material if it is of a personal nature and on non-public accounts - e.g. we are conducting an investigation into something and suspect that social media/open source material can with assist us in that investigation or assist in apprehending an offender. We should not be able to view private facebook accounts etc without any grounds or reason to do so. However material which is openly placed on the internet in a public way should be viewable by us as it would be by any other member of the public.		I have a mixed opinion on this but personally conclude that if you put something online publicly, even with the intention of it only being seen by friend etc, it is still in the public domain and should be able to be viewed as part of an open source investigation. The privacy argument is a valid one but as police officers, if there is evidence or other useful information pertinent to an investigation sitting on the internet for public view without barriers, we would be doing a dis-service to pass over it.
		I suggest there are already in place procedures to gain any information required with obviously valid and justified reasoning.	I like the idea of what we are investigating being proportionate to what we can access. If I was the gate keeper that would probably not be the case.	I think it is right that the balance should be on the side of police having to make justifications for the right to view open source information if it is of a very personal nature.
		If it is for police work/investigation then it should not be made hard to get authority by someone not around. It would be helpful if it was a tool that any investigator could use	if information is in the public domain and it assists with a policing purpose then the public should reasonably expect it to be accessed.	I think police should automatically have the facility to view this data, but any police search it needs justification. However this does not and should not necessarily include prohibitive administration. Imagine how few crimes would be progressed if an Optica application had to be completed for every PNC check!
		If it is for investigation purposes we should be able to conduct this research in order to speed up the investigation process and rule out/identify suspects faster.	This is a sensitive legal issue, which has to be carefully considered and decided upon by the legislator. A consultation process might be required to reach a decision on this matter.	Among many other factors, it will presumably be necessary to strike a balance between the rights of an individual including the individual's human rights on the one hand and the necessity to investigate into the commission or preparation of the commission of a serious crime, which might endanger the wider public or put national security at risk.
		There must be set guidelines which are kept to	if there is a level of intrusion which goes beyond this then a level of authorisation should be required.	There should be more of a debate about young people be able to comit crime and view porn on mobile smart phones