POLICING IN AN INFORMATION AGE

Jamie Bartlett, Carl Miller, Jeremy Crump and Lynne Middleton

March 2013

DEMOS

Published by Demos 2013

Third Floor
Magdalen House
136 Tooley Street
London SE1 2TU

T 0845 458 5949
F 020 7367 4201

hello@demos.co.uk
www.demos.co.uk

PREFACE

The Centre for the Analysis of Social Media (CASM) is a collaboration between Demos and the Text Analytics Group at the University of Sussex. It produces new political, social and policy insight and understanding through social media research.

CASM produces policy papers that consider the ways in which social media is affecting various aspects of public policy and politics. These papers are short, evidenced, and forward looking – raising issues and questions for further research rather than offering definitive answers.

This paper is based on a review of relevant evidence, a small number of interviews and some primary research looking into the social media following of some police forces. Future policy papers will cover social media and election campaigning, research ethics for automated data collection, and gauging public opinion via Twitter.

EXECUTIVE SUMMARY

Policing is an information intensive business. This means that changes in the way people create, share and use information present new challenges to the task of policing a democratic society.

The widespread adoption of social media is one such change.[1] Social media allows the police to engage and include the public in law enforcement in new, potentially transformative ways. But it also makes these engagements more difficult to control, and open to misuse and reputational damage. It allows the police to gather powerful, recent and possibly decisive intelligence – social media intelligence or 'SOCMINT' - in the interests of public safety. But there is a risk that this will be done in a way that is unsound, unsafe, and radically undermining of public trust. Social media is a new source of evidence for enforcement purposes, but also a new theatre of crime.

For at least the last five years, dealing with these opportunities and challenges has become increasingly important to police forces. The initial doubts which many may have had about the relevance of social media platforms to police work were largely dispelled by the August 2011 riots. Since then, police interest in and use of social media has increased rapidly against a background of greater pressure on police budgets and the beginnings of a decline in police numbers.

All forces in the UK have some presence on Twitter, with accounts for senior police officers, central communications, neighbourhood, helicopter, road and football policing teams. Some police officers tweet in a private capacity. West Midlands Police for example has accounts for individual officers, force football teams and even the police dog.[2] Other social media platforms – Facebook, YouTube, Flickr, Pinterest, Google +, Audiobook – are also used, often linked to Twitter accounts. Most forces have formal social media policies and strategies, and most use social media as a basis for investigation or as evidence.

In this short paper, we summarise the key opportunities and difficulties social media presents for engagement, intelligence and enforcement. It is far from comprehensive and offers only an overview of each. Nevertheless, it seems to us that the police will now certainly need to use social media to engage with the public, collect intelligence, and investigate crime, both on- and offline. This needs new settlements – in doctrine, resource allocation, operation, capability, regulation and strategy – that allow it to be done in accordance with the principles at the heart of the British model of policing: legitimacy, accountability, visibility, compliance with the rule of law, proportionality, the minimal use of force and engagement with the public.

Engagement

The police already use social media as a direct channel for engagement with the public. It is currently being used as a constant and reassuring contact, sharing accurate information and dispelling rumours. It can also allow citizens and the police to work together to make society safer. Both Facebook and Twitter have become highly useful means for the police to engage the public. Women make up two-thirds (68 per cent) of police forces' Facebook fans, and one third of all Facebook fans of the police are under 25. In general, the majority of both Facebook and Twitter followers of police accounts are local to that force, which suggests (although it does not prove) that these profiles are considered a useful source of local information.

Intelligence

The provision of legitimate, timely, decisive and robust SOCMINT can contribute decisively to public safety. Using social media to 'crowd-source' information is an important way of gaining valuable intelligence. 'Listening' to social media using powerful 'big data' acquisition and analytics tools can help the police spot emerging events, piece together networks and groups, discern public attitudes and improve situational awareness. More intrusive forms of intelligence collection – such as the use of intercept or covert human intelligence – may also be useful, although they will be used

less frequently. It is likely that SOCMINT will become an increasingly important source of intelligence for the police. However, it requires a clear set of guidelines and regulations to ensure it is proportionate and based on broad public consent.

Enforcement

Social media is an increasingly important public space where crime can be both committed and detected. Subject to public law, it provides new sources of evidence for criminal investigation and prosecution. Social media creates spaces where established types of crime are carried out in a new context, old offences take on new forms, significances, profiles and frequencies, and entirely new forms of crime take place.

Recommendations

There is an opportunity for British police to be world-leaders in the ethical, effective and cost-saving use of social media. To realise this ambition, three parallel developments are needed.

Firstly, there needs to be an enabling ethical, legal and regulatory framework that allows the police to use social media with the confidence that what they are doing is legally permissible, protects the reputation of their organisation and ultimately commands public confidence. The framework must be: clear, unambiguous, consistently applied across England and Wales, and with a link between enabling legislation and police practice, doctrine and procedure.

Secondly, the police must develop capability. From effective, confidence-building engagement, to reliable and trustworthy intelligence and admissible, powerful investigative and evidence-gathering work, there needs to be a sense of what works, what does not, and how performance can be measured. This is likely to require significant and imaginative technological and methodological development.

Third, there needs to be a cultural change. The police should embrace the concept of ‘co-produced safety’: actively looking for

opportunities to involve the public more in policing, whether that is the newly elected Police and Crime Commissioners using social media to inform the public about decisions and meetings, using Twitter to crowd-source intelligence by emulating the #shopalooter campaign, e-neighbourhood watch, or reaching out to groups that traditionally have been hard to contact.

To achieve this, we believe the following specific steps are necessary:

A centralised SOCMINT 'hub' should be created. The Police need to evolve and strengthen SOCMINT capabilities. A single, networked hub of excellence and a managed network of experts should coordinate SOCMINT development across different branches of the police. Structures of engagement and funding must be created to involve extra-governmental actors, especially those from industry and academia, where possible. This hub should:

- Collect, store and analyse social media data, and develop methods for use by police forces.
- Manage relationships with the major platform providers in a strategic way, for instance by reporting breaches of terms and conditions rather than taking a legal route.
- Create a structure for cooperation between police and outside expertise.
- Produce specialised training for intelligence analysts and those who will work closely with the Crown Prosecution Service. This includes the possible risks of social media use, such as the identification of personal information relating to individual officers.
- Advise on purchasing and commissioning decisions, so that individual constabularies do not purchase or lease ineffective and over-priced technologies which do not deliver any benefit.

- Review the guidance for managing very large volumes of personal data. This needs to include a storage policy for both intelligence and evidence. Social media information that is collected but not used for intelligence or on-going investigation purposes should be discarded safely and quickly.

- Evaluate the effectiveness of methods and techniques that are applied across the forces.

The Home Office should create a clear, publicly argued framework for the collection and use of SOCMINT, based on the existing Regulation of Investigatory Powers Act (RIPA). The police will sometimes need to access social media for intelligence work, in a variety of intrusive and non-intrusive ways. But as it stands, the legal basis for SOCMINT is not clear. The collection and use of intelligence from social media must be placed on a firm regulatory basis. We believe RIPA can be used to regulate and manage different types of SOCMINT:

Open source SOCMINT

This is intelligence collected from open, publicly available sources where no private information is collected about an individual, (unless the user would have no expectation of privacy), and the methods of collection do not involve deception or interception. Therefore, there is no interference with Article 8 rights to privacy, and no authorisation through RIPA is needed. It includes:

- Access to open source Twitter information, via the Application Programme Interface (API).

- The use of listening-in technologies that do not result in the collection of any private information about individuals, in which data are aggregated and anonymised. This includes general trend analysis or sentiment analysis.

However, the use of open source SOCMINT should still be proportionate, necessary, and minimal in scope.

Directed surveillance SOCMINT

When private information about a person is taken from a public domain where there is a reasonable expectation of privacy, authorisation is required under RIPA measures that cover directed surveillance. This means the surveillance must be signed off by an 'authorising officer' (usually a superintendent for the police), only applicable for certain statutory purposes, and based on a proportionality & necessity test.[3] For SOCMINT, directed surveillance would include:

- Building a detailed profile of the interests, views, and behaviour of a single named individual from openly available sources.

- Social network analysis that identifies individuals and seeks to place them as part of a network. This includes network building through 'crawlers' and other 'bots' that identify individuals who are not of interest to the authorities.

Covert human intelligence sources SOCMINT

If the police establishes or maintains a relationship with a person for the covert purpose of obtaining information about them, or to get access to information about another individual using social media, it is classed as a covert human intelligence source. Authorisation is required under RIPA, through existing measures that cover Covert Human Intelligence. This means it must be signed off by an 'authorising officer' (usually a superintendent for the police), only applicable for certain statutory purposes, and based on a proportionality & necessity test. If combined with intrusive surveillance, it would require authorisation from the Secretary of State.[4] For SOCMINT, covert human intelligence would include :

- Creation of fake/pseudo/anonymous social media accounts (sometimes called "Ferret" accounts on Facebook) in order to join a closed group or chat room.

- Any direct interaction in any forum – open or closed – in which an officer seeks to elicit information, if they are not explicit about their real identity.

Intercept or intrusive covert surveillance SOCMINT

Intelligence gathered from social media that makes available the content of a communication, while it is being transmitted, to a person other than the sender or intended recipient, by monitoring, modifying or interfering with the system of transmission. This falls under Chapter I of Part I of RIPA, which requires a warrant from the Secretary of State. In the case of SOCMINT, some activities may also be considered covert intrusive surveillance, which requires an authorisation by a Chief Constable with the approval of the Surveillance Commissioner (unless the case is urgent), although current RIPA guidelines on intrusive surveillance mainly cover residential property, and not internet-based communication.[5] For SOCMINT, intercept/intrusive covert surveillance would include:

- The use of any crawler, spider, scraper, or any other automated system that breaches a robot.txt restriction in order to access data from a server without the permission of that server (regardless of the type of information accessed).

- Any data coming from closed accounts, or access to accounts or groups where any restriction has been placed limiting the access (for example 'friends only' settings on Facebook), even if the group involved is extremely large.

- Accessing direct messages (DMs) on social media where the information is available only to the individuals involved.

Each constabulary should have a single dedicated, operational lead for social media to integrate the various applications. This role should include:

- Integrating social media monitoring into control centres.

- Managing possible jurisdictional issues, such as who takes responsibility for investigations where it is unclear where the offence took place.

- Acting as a single point of contact to manage and filter social media requests and conversations, which should include 24 hour staffing of social media accounts.

- Taking responsibility for the correct use of social media accounts, managing engagement, crowd-sourcing intelligence collection (such as the #shopalooter campaign), reviewing existing capability, and neighbourhood engagement (such as e-neighbourhood watch).

- Managing the public's expectations of what 'social media policing' can and cannot achieve, such as investigating reported trolling, cyberbullying and low-level identity theft.

Inevitably, as the way we communicate changes, so must the ways in which we maintain law and order. However, digital freedom and liberty are increasingly important for citizens, and some aspects of policing work are not amenable to the norms and mores of social media. We therefore recommend that the police proceed with care. They should not underestimate the potentially transformative power of social media to their work, nor underestimate the legitimate concerns citizens have about misuse. The use of social media should be guided by the same principles that underpin all police activity - public confidence and legitimacy, accountability, visible compliance with the rule of law, proportionality, the minimal use of force, and engagement with the public.

THEME 1: ENGAGEMENT

Opportunities

The British police are already Europe's leaders in the use of social media, especially in community policing.[6] Most frequently, this engagement is either a strategic one, managed by a central communications team, or one that is focused on local communities by neighbourhood policing teams. According to one researcher, 98 per cent of British police forces have a corporate Twitter account, with an average of 18,000 followers; 96 per cent have a Facebook account; and 94 per cent have YouTube accounts, with a total of more than 3,600 videos uploaded. The huge spike in use came, perhaps unsurprisingly, after the 2011 riots.[7] The Association of Chief Police Officers (ACPO) has invested effort in commissioning good practice guidance and information sharing activities for practitioners.[8]

There are a number of opportunities for using social media to engage with the public effectively. Many, at core, require a shift in philosophy from treating social media as a one-way messaging channel, to treating it as a platform which allows more durable communities to form with the police at their heart.[9] As democratically elected Police and Crime Commissioners look to extend their engagement with the public this is important for them to consider.

Sharing information

Most simply, social media can be, and often is, used to inform the public rapidly and directly. Possible applications are as wide and diverse as policing itself, from reporting success and providing reassurance, to promoting community activities and delivering statements.

Reporting success

Eastbourne Police *@Eastbournepol*

Man arrested in connection with Eastbourne Ladbrokes robberies: *http://bit.ly/ZuVMx8* (20 Feb 2013)

Metropolitan Police *@metpoliceuk*

A convicted drug dealer from ***#Hackney*** has had £40k of assets seized *http://bit.ly/109Vxg5* (16 Jan 2013)

Providing reassurance

Brighton City Police *@BTNCityPolice*

No Burglaries, Robberies, Sexual offences or Serious assaults in *#Brighton* city centre over night. (20 Feb 2013)

Brighton City Police *@BTNCityPolice*

Helicopter will be landing in East *#Brighton* Park shortly nothing to worry about, collecting crew members for their next job. (19 Feb 2013)

Promoting community activities

Stoke Police *@policingstoke*

We are giving information today to the City Council task and finish group re the night time economy. You can have your say at council web. (23 Jan 2013)

Leicester Police *@CityCentreLPU*

Come & meet local beat officers today at Bishop Street, *#Leicester* Library from 10am until 1pm! Tell us your local issues & say hello!(20 Feb 2013)

Delivering statements

GMP Failsworth *@GMPFailsworth*

We have launched the myGMP consultation process on our website http://www.gmp.police. Click on the link to see... *http://fb.me/1yGjbkzru* (21 Feb 2013)

WestYorkshire Police *@WestYorksPolice*

#police Help needed identifying this person in North West Leeds: In relation to the crime of Cri... *http://bit.ly/Y6pDyu* *#caughtoncamera* (20 Feb 2013)

Dispelling rumours

A more controversial method of engaging with the public is to dispel rumours and conspiracy theories, for instance by proactively intervening in discussions and conversations. The viral, mimetic and networked nature of many social media platforms allows exaggerated, false and malicious information to spread very rapidly.[10] During the August riots of 2011, nonsense claims about tigers in Primrose Hill and the Army deploying at Bank swept through Twitter, propelled by a series of credulous retweets. In response, some forces used social media to debunk such rumours. Staffordshire Police have been using Twitter for rumour-dispelling activities since January 2010, particularly in relation to monitoring and dealing with English Defence League protest and counter-protest.[11] The most effective debunking messages are crafted to be as appropriable and shareable as the misinformation they seek to confront. For example, West Midlands Police Force used social media and particularly Twitter to counter rumours of an attack on the police station by posting 'twitpics' of officers standing outside the station. Nottinghamshire Police used social media in a similar way to provide reassurance and appeals for information during the August 2011 disorder.[12]

'Co-produced safety'

There has been a clear recognition in recent years that including a large number of different actors in public security makes sense. The British counter-terrorism strategy relies on the active engagement of citizens.[13] In the US, the gang-prevention initiatives that work are those that have 'all-community' involvement from the police, social support services, charities, youth groups, local churches, parents' organizations, rehabilitation centres and schools.[14]

There is great potential for the police to create and curate networks of citizens cooperating to keep their society safe. Indeed, there are already examples of this 'co-production' of safety and justice, often at the instigation and insistence of the civilian participants, not the police. The Greater Manchester Police's #ShopaLooter campaign spread to the rest of the country, as thousands tweeted and

retweeted screenshots of and links to alleged looters bragging about their exploits, using the 'shopalooter' hashtag. Many citizens had already taken to Twitter to search for and collect evidence of criminal behaviour. Similarly, in the aftermath, citizens organised themselves using #riotcleanup, and staged public demonstrations to condemn the criminality and the violence.

Reaching new groups: Facebook and Twitter

Most police forces have Facebook pages. The 24 UK police forces with the most 'liked' Facebook pages between them have been liked by 302,100 people based in the UK.[15]

Interestingly, the demographics of these people show that 32 per cent are men, while 68 per cent are women. 32 per cent are aged 25 or younger, 40 per cent are between 26 and 39, and 27 per cent are between 40 and 59. Only three per cent are 60 or over. Similar figures obtain for the Greater Manchester Police, which has the single largest Facebook fan base. The majority do appear to be local people – 83 per cent live in Manchester or towns within a 25 mile radius of Manchester, and 57 per cent live in Manchester itself. As above, around one quarter are under the age of 25.[16]

In terms of engagement with Facebook content, the Metropolitan Police Service Facebook page is a useful example. From the 1st – 18th February 2013, the Metropolitan Police made 17 posts, of which 14 contained multimedia (13 photos, one video) and three were link shares. These posts had an average of 115 engagements each (meaning a comment, share or like). Of all engagement, there were 222 comments, 1,486 likes, and 253 shares (averages per post: 13 comments, 87 likes, 15 shares).[17]

As of this report being published, the Metropolitan Police Service Twitter account has 93,924 followers. Of these followers 19 per cent are judged by the social media analytics 'fakers' tool to be fake or spam accounts, not registered to genuine individual users – therefore 76,078 users are active. [18] Location tools give a picture of the proportion of followers that are in the UK and within the

bounds of the Metropolitan Police area: 51 per cent of account followers are in London and 76 per cent in the UK.[19]

Similar figures were found for the Greater Manchester Police Twitter account, which has 120,177 followers: 11 per cent are judged to be fake or spam accounts, therefore 106,958 users are active. Of these, 56 per cent are in the Greater Manchester area and 89 per cent are in the UK.

There are also several smaller accounts. West Midlands Police, for example, lists 157 separate Facebook accounts. These include official police accounts for local towns and boroughs, University and football club accounts and those of individual officers. The Aston Neighbourhood Police Twitter account has 128 followers (six per cent are judged to be spam, so 120 users are active individuals). A similar measure of the geographic location of the followers of Aston Police shows 80 per cent to be in the Birmingham area, and 95 per cent in the UK.

Challenges

Any form of appropriate engagement with the public on social media needs to manage a number of risks. The established culture of policing is necessarily based on command and control, hierarchy and operational security. It is conditioned by the role of the police as agents of the criminal justice system and hence the need to preserve the integrity of evidence and the rights of suspects and victims. These cultural values often sit uncomfortably with the openness, informality and public nature of communications on social media.

Controlling social media communications

The first challenge is setting the right balance of central control. Police forces have understandably sought to limit the risks of this new environment by issuing guidance and establishing internal control procedures.[20] Police force policies therefore usually include guidance which requires police officers to protect the reputation of the force and to pay proper attention to operational considerations such as protecting the identities of victims and witnesses, protecting

the integrity of current operations and avoiding comment which might be prejudicial to legal proceedings. Policy and guidance is enforced in a number of ways. Forces typically give the communications directorate control over who can set up an official Twitter account. Typically, officers are required to undergo a training course before they are given control of an account. Once accounts are set up, force communications teams have various means of supervising what officers are doing. Thames Valley's corporate communications team monitors all their accounts on a daily basis. West Midland's corporate communications department holds the passwords to all accounts and it reserves the right to delete or insert material without consultation. There are further mechanisms in place to control more sensitive material that might be referred to in social media. Thames Valley requires that any picture on Twitpics be authorised by those police officers who appear in it.

The tweeting officer typically needs to have a general list of things to do and not to do. Underlying these requirements is a wish to ensure that officers apply a similar set of judgments to what goes on Twitter as they would to a public spoken utterance, especially one that was being reported in the media. Most forces' guidance encourages officers to follow partner organisations, local businesses and (with due regard for political neutrality) opinion formers, and to reply to questions and inquiries promptly. The monitoring of the Twitter account then becomes a source of local intelligence. Personal opinions about politics, comments about other stories in the news and criticism of other people are discouraged.

Given the extent of police activity on Twitter, the number of occasions in which serious errors have been reported is small. Most recently, four out of 45 officially accredited 'tweeters' at Northamptonshire police have been stripped of this duty following concerns that their tweets might breach the Data Protection Act for both investigative and legal reasons.[21] Officers from Nottinghamshire Police have been stripped of their accreditation to tweet following concerns that their Tweets may breach the Data Protection Act,[22] while an investigation is underway into one

Sergeant in Walsall based on the content of his Tweets.[23] Ensuring that officers have the freedom to engage in the medium without causing damage is a balancing act, and there is certainly a considerable amount of media interest in the subject which makes this challenge more difficult. When a Police Community Support Officer in Exeter was given words of advice by the Devon and Cornwall Police about the content of her tweets, the story received coverage in the national press.[24]

Two-way communications

However well controlled, the opening of direct channels of communication between the public and the police poses inherent risks. Responsibility rests with the police to respond to every 999 emergency call, and, with less degrees of urgency, to other non-emergency forms of contact by the public. Currently, police forces have taken the view that tweets directed at an official account should not be treated with the same degree of urgency as other forms of communication – indeed, most police sites on Twitter contain a warning not to use the channel to report crime. Twitter feeds are not routinely staffed 24 hours a day, or integrated into force control centres. Nevertheless, a number of forces are reporting a significant increase in the amount of information requests coming to them through social media. There are not, as far as we know, systems in place to manage and filter these requests.[25] While this is not a significant problem yet, we anticipate it might become one in the near future.

Wider disruptions to communications strategy

Social media can also disrupt other forms of communication and engagement. Evidence submitted to the Leveson Inquiry made it clear that social media is changing expectations and requirements, and raising questions about the Police Force's whole communications strategy.[26] The response is challenging both for the Press and for Police Communications Officers. Journalists and reporters are increasingly finding breaking stories online, and go to the police for verification before the force is ready, or has taken the required measures, to confirm or deny.[27]

THEME 2: INTELLIGENCE

The concept of intelligence-led policing underpins all aspects of police work, from community policing to organised crime and terrorism. This approach relies on intelligence to inform decisions about priorities and tactical options. At the point of inception in the 1990s intelligence-led policing used criminal intelligence and crime analysis in a strategic manner, with intelligence no longer used exclusively as a means to develop case-specific evidence. Following the London Riots, the Police publically asserted that security planning for the London 2012 Olympic Games was "intelligence-led".[28] This philosophy is enshrined in the 2000 National Intelligence Model (NIM) a conceptual model which is used across the Police Service and is applicable across all aspects of policing demonstrating the centrality of intelligence led policing today.[29]

Opportunities

Intelligence has been defined as any information that can improve the quality and timeliness of decision-making by reducing ignorance. Increasingly, open source information is considered an extremely valuable and important source of intelligence, particularly as more content is created and shared. Social media's possible applications and potential contribution are beginning to be understood, but can in cases be decisive, and include learning about potentially violent group activities (the English Defence League, for example, used Facebook to arrange its demos), criminal behaviour, signs of disorder, community tension and more.

Social media offers new opportunities to crowd-source intelligence. A number of sporadic successes have established the ability of the crowd to offer effective contributions to intelligence when directly solicited. During the 2011 riots, a West Midlands Police website allowed citizens to post messages and questions, allowing the police to build up a picture of the situation on the ground in real time, as well as allowing people to identify pictures of suspects placed on the site.[30] Following the 2011 riots, police uploaded photos to a Flickr Stream and a dedicated website that compiled images of people thought to be involved in looting. As a result 770 people were arrested and 167 charged. Furthermore, up to 2,800 images were

uploaded to a smartphone app – Facewatch ID, a partnership with Crimestoppers – which allowed users to sort the images via postcode and then inform on those they recognised by sending a name and address to the police. The app also included 2,000 or more images of people wanted for offenses unconnected to the riots.[31]

The explosion of social media communication by the public in open or quasi-open spaces also presents opportunities for improved intelligence and information for police. These possibilities are set out in detail in *#Intelligence* (Demos 2012). These digital-social spaces are the largest, constantly refreshing testament to human behaviour ever created. Our increasing ability to collect, understand and therefore harness these spaces as sources of information promise to make SOCMINT-as-listening an important part of the police's intelligence framework. The uses span from understanding public attitudes about the police, identifying tipping points and thresholds to violence, to following public responses to prominent speeches, announcements and court cases. For instance, SOCMINT systems are increasingly able to cluster social media output to indicate and describe unfolding offline events in real time. A series of academic papers under the new discipline of 'Twitterology' has shown that, while the majority of Twitter traffic occurred after an event had been reported by a mainstream news outlet, 'bursts' of tweets indicating a significant event often pre-empt conventional reporting. Social media traffic analysis could allow for a more rapid identification of events than traditional reporting mechanisms. With the application of geo-location techniques this could lead, for example, to a constantly evolving map showing spikes in possible violence-related tweets. This would facilitate a faster, more effective, and more agile emergency response.[32] Other capabilities include the use of network analysis to better understand groups and relationships[33]; to measure the early signs of community level concerns about a subject or issue; to give demonstration size predictions[34] and to provide early indications and situational awareness of natural disasters to emergency responders.[35]

In addition, there are the more traditional types of intelligence collection, such as the interception of communications or the use of covert human intelligence sources to extract information. This could include putting the social media presence of criminal suspects under surveillance; cross referencing such individuals' accounts; identifying accomplices; uncovering assumed identities; covertly joining closed social media networks or groups; identifying criminal networks that operate through social media sites; and the provision of social media content suspected of being evidence of a crime to the Crown Prosecution Service.

Challenges

SOCMINT, like any new type of intelligence, faces a number of formidable ethical, operational, and technological challenges.

Legal/regulatory system of SOCMINT

Like all intelligence work, SOCMINT must be carried out within a legal framework. This framework must provide a sound, publicly argued legal footing that provides clarity and transparency over SOCMINT use, storage, purpose, regulation and accountability.

As it stands, RIPA 2000 Parts 1 and 2 provide the legal basis in the UK for the collection of intelligence likely to involve accessing private information. SOCMINT did not exist when RIPA 2000 was conceived and it is hard to simply slot into the existing categories and typologies established by RIPA, or that might be covered by data protection legislation. There are a number of reasons why SOCMINT presents challenges to the current framework. Although it covers both open-source data and closed networks, the distinction is not always clear. For example, Facebook accounts and groups often have varying degrees of openness, and different platforms often have quite different terms and conditions and norms of use that might determine the degree of intrusion

Because information is open source, it does not necessarily follow that the police should collect and analyse it. Proportionality and necessity still apply because the police also has a duty to uphold the economic and social well-being of the nation, which includes a free

and open internet: and expectations of privacy – one of the key factors in determining authorisation decisions – are not always obvious. Moreover, social media analysis software and tools allow for far greater surveillance than ever before, with concomitant risks and opportunities. The increased use of automated software to collect and analyse information (inevitable in the age of terabytes of unstructured data) poses additional risks of misuse. Public attitudes towards data sovereignty and privacy (even on open platforms) change quickly, and there is a reputational risk if law enforcement agencies are seen to be 'snooping' online.

The lack of legal clarity over the use of SOCMINT by government is a looming legal and reputational problem. Privacy International, for example, has launched a series of Freedom of Information requests about the Metropolitan Police's use of social media analysis, which have not yet been answered. Similarly, Big Brother Watch has raised concerns about plans like Westminster Council's 'Your Choice' programme, which it worries could breach citizens' privacy by accessing their communications via social networking sites.[36] [37] [38] Without a clear set of guidelines and a framework for the collection and use of various types of SOCMINT, and how they map onto existing RIPA definitions (or indeed entirely new categories), there is a danger of serious and sustained damage to public trust. Below, we set out a proposed way to regulate SOCMINT through the existing categories set out in RIPA.

Development of SOCMINT capability

Following the August 2011 riots the police acknowledged that they had been insufficiently equipped to gather intelligence with social media. Social media did not fit into their systems of receiving, corroborating, prioritising and disseminating information, and therefore was not properly acted on. Her Majesty's Chief Inspector of Constabulary noted, 'With some notable individual exceptions, the power of this kind of media (both for sending out and receiving information) is not well understood and less well managed'.[39]

Yet for information to be considered 'intelligence' it needs to meet certain thresholds of how it is gathered, evidenced, corroborated,

verified, understood and applied – evidentiary standards. Different sources and kinds of intelligence have developed signature ways of meeting this challenge. Open-source intelligence (OSINT) triangulates reliable sources; human intelligence (HUMINT) might consider the track record of the agent; imagery intelligence (IMINT) needs to pay attention to the technical characteristics of the collection platform; and signals intelligence (SIGINT) would need to understand the context of the language used. All source intelligence assessments try to get an overall picture on the basis of these different types and the reliability of the contribution.

To be able to inform important decisions, either strategic or operational, SOCMINT must establish its own approach to secure these evidentiary thresholds. Many challenges stand in the way of SOCMINT being able to do this, but three in particular we consider to be critical: sampling, analysis, and spotting counter-intelligence.

Extrapolations depend on the quality – especially the representativeness – of any research sample collected. The social sciences have not developed an approach to robustly sampling social media data sets. At present, social media research is obsessed with size: collecting enormous samples (something that computational approaches are good at delivering), rather than representative ones. The most readily available or easily accessible – rather than the most representative – data are collected. Collecting a comprehensive (rather than representative) set of data on a subject using various key word and automated topic identity approaches is also very difficult. The social sciences are concerned with causal significance and the generation of more general theory, whilst current social media analysis has not moved beyond the raw, descriptive enumeration of social media phenomena or uncritical readings of the 'obvious' implications of the data.

At some point researchers want to know 'why' as well as 'what'. The intent, motivation, social signification, denotation and connotation of any utterance are dependent on the context of the situation. So the accuracy of any interpretation depends on a very detailed understanding of the group or context that is being studied. However, because automatic data collection is required to process

the sheer volume of data now available, many of the contextual cues – the thread of a conversation, information about the speaker, the tone of the utterance and the information about the speaker – are often lacking in analyses of social media data. The act of 'scraping' a social media platform – such as collecting Tweets or Facebook posts – often by definition de-anchors a text from its natural setting. Some studies for example argue for an 'online disinhibition effect' – that the invisible and anonymous qualities of online interaction lead to uninhibited, more intensive, self-disclosing and aggressive uses of language.[40]

Intentional misinformation – sometimes referred to as counter-intelligence – is also likely to become an issue for the police. Already there are a considerable number of non-authentic and fake accounts (sometimes called 'sock puppets') on many social media platforms. Facebook recently revealed that seven per cent of its overall users are fakes and dupes.[41] Some of these fakes have been used for intelligence collection by non-government agents, and others have misled highly specialised experts.[42] For example, Amina Abdallah Arraf al-Omari, the so-called 'Syrian-American lesbian', living in Damascus, shared her on-the-ground insights in compelling detail on her blog 'A Gay Girl in Damascus'. She was later revealed to be a PhD student at Edinburgh University.[43] 'Astroturfing' – the technique of creating online personas who masquerade as authentic, ordinary individuals – has become something of an industry in itself. Some experts estimate that about a third of all online consumer reviews are fake.[44] [45] It is our view that one core aspect of any SOCMINT capability will be the ability, both analyst and automated-led, to weed out false and misleading information.

Given these current weaknesses, it is likely there needs to be greater investment in human and technology capabilities to create a new academic inter-discipline fusing technological capability and humanistic understanding together: social media science.

A PROPOSED REGULATORY FRAMEWORK FOR SOCMINT

The legislation that governs UK public authority use of covert techniques likely to obtain private information is the Regulation of Investigatory Powers Act 2000 (RIPA). The general principles of necessity and proportionality run through RIPA, meaning the more serious the intrusion into someone's privacy (Article 8 of the Human Rights Act), the fewer agencies that can do it, and for fewer purposes. When an agency applies for a RIPA warrant, a suitably senior authorising officer decides if the proposed measure meets the proportionality and necessity test.[46]

The police will sometimes need to access information from social media for intelligence or insight. RIPA was written before social media, and it is not always clear how it applies to SOCMINT. Making a decision about whether certain types of SOCMINT might require an authorisation under RIPA is not easy: some SOCMINT is more intrusive than others.[47] Judgements rely upon a number of distinctions and assessments – from what is proportionate to what is a private space – that are contextual, mutable and a matter of degree. In respect of SOCMINT, this is extremely difficult indeed. As general conceptions and expectations of privacy change, it is not clear what is private information and what is not. RIPA currently defines surveillance as 'monitoring, observing or listening to persons, their movements, conversations or other activities and communications,' stating it to be covert if it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place, as defined in section 26(9)(a) of the 2000 Act[48]. (This is why CCTV – open, visible, widely known about – is considered to be overt, and does not ordinarily require RIPA authority). One of the strengths of listening-in technology is that it captures conversations in natural settings, and although not necessarily intentionally covert, it is often done without the consent or knowledge of those being monitored. Deception can also take new forms. For example, signing into a social media platform through an anonymous account to listen might be considered deception, even if it requires little active deception. It is also increasingly easy to create believable fake 'ferret' accounts which can collect information, including the use of automated 'research bots' that mirror other users' behaviour.

We believe that the new types of SOCMINT available potentially fall under the four categories: 'open SOCMINT' (which would not require authorisation) and three existing categories of intelligence work currently set out under RIPA (directed covert surveillance; covert human intelligence source; and intercept). Below we set out which types of SOCMINT might fall under each of these categories. This is not legal advice, but merely a series of suggestions as to how both existing legislation and individual decisions by authorising individuals might approach SOCMINT collection and use.

Open SOCMINT

Intelligence collected from open, publicly available sources, where no private information is collected about an individual (unless the user would have no expectation of privacy), and where the methods of collection do not involve deception or interception, creates no interference with Article 8 rights to privacy. Applied to SOCMINT, this would include:

- Volunteered crowd-source intelligence through direct and explicit solicitation. This should be employed wherever possible in preference to 'listening in' technologies and techniques.

- Listening-in technologies that do not result in the collection of any private information about individuals, where data are aggregated and anonymised. This includes: general trend analysis, hot-topic analysis, and generalised population sentiment analysis conducted using machine learning.

- In some cases, private information (such as names, interest, location) can be collected, but only if social media users have no reasonable expectation of a right to privacy, because they understand this content is likely to be shared and used. That condition is met if any terms of agreement establish that content uploaded is public and will be made available through an Application Programme Interface access (such as Twitter, which makes it clear that it will actively encourage sharing and consequently, data collected from open Twitter accounts would not require authorisation). In addition, no privacy blocks or walls (often effected through the use of robot.txt restriction) or password requirements exist.

- Network analysis through the use of 'crawlers' or 'spiders' (automated programmes to map a network of individual accounts), providing no individuals are named or private information about an individual is collected, and where API access is granted through robot.txt, and is made clear on the terms and conditions that data are shared.

- Where a profile needs to be created in order to access even publically available information (such as through Facebook), this is still considered open if that data is also available through direct access to the API. However, in such cases, the data should be accessed through the API rather than manually scraped using an anonymous profile, as the creation of anonymous profiles increases the likelihood that covert human intelligence methods might need to be authorised.

- General and speculative trawling (meaning non-specified searches based on keywords/terms) of platforms that are open, such as Twitter, but may be subject to other types of limits and oversight to encourage greater targeting and accountability.

However, considerations of reputation, public acceptability and proportionality should inform any decisions taken in respect of open SOCMINT. Even if it is legally acceptable, the use of large scale, automated social media analysis at the population level might not command public confidence. Therefore, agencies undertaking this type of research work should try to conduct open SOCMINT work according to good ethical and professional research standards:

- Be explicit and public about the research aims and methods used, where possible.
- Take due considerations of the norms of the platforms (such as whether or not the platforms tends to be used to divulge what might be reasonably considered as private information). Not all 'open' platforms have the same reasonable expectations of the user.
- Consider whether the measures taken might reasonably be seen as proportionate by those potentially monitored, and whether they could be defended as such.
- Assess if any measures might undermine the existence of a free and open internet, which would cause damage to the economic and social well-being of the nation.
- Assess whether such measures are an effective use of public money.

Directed covert surveillance SOCMINT[49]

According to RIPA, directed covert surveillance covers surveillance which is covert but not intrusive (i.e. not taking place in a private residence) but is likely to result in the obtaining of private information. Private information can be quite varied in type and includes any information relating to a person's private or family life. Under current RIPA guidance, while there is a reduced expectation of privacy in public places, covert surveillance of a person's activity in public may still result in the obtaining of private information. As such, some SOCMINT will legitimately fall under directed covert surveillance because a) much private information is shared on public domain social media spaces; b) reasonable expectations of privacy vary; and c) SOCMINT often uses listening-in technology such as scrapers, which, whilst they might not be 'calculated' to be covert, are usually designed in a way to be unseen. As such, the following might fall under directed covert surveillance and would thus need to meet the same requirements in terms of authorisation (for the police, the authorising officer needs to be a superintendent), purpose, and authorised agencies, as set out under RIPA 2010 (Directed Surveillance and Covert Human Intelligence) Order. A proportionality and necessity test needs to be considered by the authorising officer. Directed covert surveillance using SOCMINT could include:

- Building a detailed profile of the interests, views, and behaviours of a single named individual from openly available sources. While this might not apply on certain platforms (principally Twitter), where a profile is built from multiple social media platforms and accounts, especially where it requires

cross-referencing profiles through either automated or manual user name recognition techniques, this might be reasonable deemed as directed covert surveillance. What are known as 'private life considerations' can arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. As discussed earlier, some of the technological advances make this more likely to be a risk.

- The collection and use of information about individuals from a public source which, although technically open, might have the reasonable expectation among users that it is a private conversation, and where private information is shared (such as small chat room forums).

- Social network analysis that identifies individuals, and seeks to place them as part of a network, including where network building identified individuals that are not of interest to the authorities.

Covert Human Intelligence Sources (CHIS) SOCMINT

Under Part II of RIPA and the RIPA 2010 Order, a person is a CHIS if he establishes or maintains a personal or other relationship with someone for the covert purpose of obtaining information about them, or to get access to information about another individual and covertly discloses that information. Unlike directed surveillance, which relates specifically to private information, authorisations for the use or conduct of a CHIS do not relate specifically to private information, but to the covert manipulation of a relationship to gain any information. Therefore, there are certain instances of SOCMINT which might reasonably be deemed as being obtained through use of a CHIS, and would thus need to meet the same requirements in terms of authorisation (for the police, the authorising officer usually needs to be a superintendent), purpose, and authorised agencies, as set out under RIPA 2010 (Directed Surveillance and Covert Human Intelligence) Order. A proportionality and necessity test needs to be considered by the authorising officer. CHIS using SOCMINT could include:

- Creation of fake/pseudo social media accounts (sometimes called 'Facebook Ferret' accounts) in order to join a closed group or chat room. This includes cases in which an individual joins using a blank or anonymous account.

- Any direct interaction in any forum – open or closed – in which an officer seeks to elicit information where they are not explicit about their real identity.

- Joining a group silently (i.e. not creating a profile but using a blank or anonymous profile) in order to join groups to listen to conversations. This might not always be considered 'deception', as much will depend on the forum.

Intercept or intrusive covert surveillance SOCMINT

Intelligence gathered through making available the content of a communication, while it is being transmitted, to a person other than the sender or intended recipient, by monitoring, modifying or interfering with the system of transmission falls under Chapter I of Part I of RIPA. Intercept covers postal services and telecommunications systems, which includes Internet communication. Although social media is not mentioned in any part of RIPA, some potential SOCMINT capabilities could reasonably fall under the intercept sections of RIPA. Because it is deemed the most intrusive type of intelligence, fewer agencies can do it, and for a more limited number of purposes, including in the interests of national security.[50] As set out in the Act, only very senior officials can make a request, and a warrant must be issued by the Secretary of State. The following types of SOCMINT might fall under intercept as far as they meet the statutory definition of interception under RIPA. (Note: it is also plausible to consider several of these types of SOCMINT as intrusive covert surveillance, rather the intercept, although RIPA guidance on intrusive covert surveillance currently covers primarily 'residential' property. Intrusive covert surveillance requires authorisation from the Chief Constable with the approval of a Surveillance Commissioner, unless the case is urgent).

- The use of any crawler, spider, scraper, or any other automated system that breaches a robot.txt restriction in order to access data from a server without the permission of that server (irrespective of the type of information it is seeking).

- Any use of keyloggers or 'trojans', to find passwords to social media accounts in order to access and monitor communication.

- Any data coming from closed accounts, or access to any account or group where a restriction has been placed limiting the access (for example 'friends only' settings). This means that an explicit decision has been made to limit the access of outside parties and thus can be considered a 'private communication' even if the group involved is extremely large.

- Any data coming from closed and password protected chat rooms or forums (where a CHIS was not employed).

- Interception of Direct Messaging (DMs) between two or more individuals that are only accessible to those individuals.

THEME 3: ENFORCEMENT

Social media has created a new theatre of criminal activity and investigation. In making the ability to conduct a public conversation easier, Twitter has also made it easier for people to commit a whole range of offences of incitement, libel and hate crime. Facebook has been used to coordinate contract killings, boast about serious animal abuse, conduct cyber-stalking, plan sexual assaults, breach court orders and cause distress through anti-social 'trolling'.

There has been a recent spate of activity surrounding convictions on Twitter and social media more generally. Enforcement of these 'spaces' is often regulated by Section 127 of the Communications Act 2003, which makes it an offence to use public electronic communications networks to send messages that are 'grossly offensive'. The number of people convicted each year under Section 127 of the Act has expanded exponentially from 498 in 2007 to 1286 in 2011. There are several other pieces of legislation that have been used in prosecuting cases, including laws regarding libel and defamation (such as the current case of Lord McAlpine suing Sally Bercow), and contempt of court. The end of 2012 witnessed a significant debate as to whether blogging on social media constituted 'publishing' and therefore would be subject to various laws relating to copyright, libel and defamation. The existing legislation for social media offences is currently being reviewed in order to provide guidelines that will ensure 'decision making in these difficult cases is clear and consistent' – with interim guidance having been set out.[51] Moreover, it is not clear whether social media platforms would be subject to the codes and conditions of the recently proposed Royal Charter set up following the Leveson Inquiry into press conduct.

Opportunities

New evidence

Social media offers a new source of evidence for prosecution and enforcement, as illustrated by the case of Michele Grasso. Grasso is a Sicilian drug dealer who had successfully evaded arrest since

2010. However, his social media activity proved his ultimate downfall, when he posted pictures of himself at London's Madame Tussauds museum,[52] and included a photo and the name of the restaurant at which he was working. This ultimately led to his arrest and deportation by British Police earlier this year.

In 2009, Strathclyde Police launched *Operation Access,* which used social networking sites such as Facebook to uncover criminal activity by identifying weapons carriers. As part of the programme, police officers searched through images to find users who had posted pictures of themselves with weapons. The Superintendant in charge of the operation stated that as a result, 400 people had been questioned.[53] Similar work – collecting valuable evidence on criminal activity such as illegal gun ownership – has been undertaken successfully elsewhere.[54] Social media has also presented significant opportunities in cases of Tort rather than Criminal Law. For example, Graham Loveday, a former lorry driver who claimed he was unable to drive following an incident in 2006, was found to be claiming unlawfully as a result of information on his Facebook profile.[55] Further, one recent report suggests that al-Qaeda and related groups are increasingly using social media for their activity: 'it is only a matter of time before terrorists begin routinely using Twitter, Instagram and other services in ongoing operations'.[56]

Indeed, criminals have been known to trip themselves up as a result of indiscretions on Facebook, as have witnesses. According to one leading QC, 'it is accepted in criminal law that remarks made on these [social media] which are inconsistent can be put to the witness as inconsistencies in evidence or as evidence of bad character'. [57]

Internationally, the potential to use social media in such ways has already been harnessed. In August 2011, the New York Police Department launched a new unit with the primary responsibility of tracking criminals on Facebook, MySpace, Twitter and other social networking sites.[58] Similarly, in Germany, police have begun to use social media in manhunts, for instance by circulating CCTV stills on Facebook.[59]

Despite jurisdictional difficulties that still plague enforcement – such as the removal of illegal or highly offensive material (see below) – there are considerable opportunities for better engagement with Internet Service Providers. Many ISPs are not the traditional companies police are used to working with. However, ISPs usually have a vested interest in ensuring their users follow their terms and conditions. There is, it appears, a general shift towards companies taking greater responsibility for educating customers about 'nettiquette', building useful filter systems, and encouraging more community policing of material and reporting of material that breaches terms and conditions. There is, we believe, an opportunity for the police and industry to work together to share ways to do that.[60]

Challenges

Resource limitations

The advent of social media has not only created new offences with which the police have to contend and new spaces for the police to visibly enforce the law, but the nature of social media has also increased the number of offences, posing issues of discretion, workload and resources.

The police may find themselves unable to investigate all the cases reported to them. Lincolnshire Police revealed that they had experienced 3437 incidents of Internet trolling since 2009, and over the same period Dorset Police noted a twofold increase in the number of cases or investigations resulting from messages posted on social media. This mirrors a 98 per cent increase in Government 'take down' requests to Google over the last year.[61] One recent case involving prolonged Internet trolling, for example, was not investigated because of the impossibility of investigating all trolling instances – of which there are thousands. [62] Trolling can range from insignificant to very serious. Last year Internet trolls were blamed for the suicides of 15 year olds in Birmingham and Cheltenham,[63] and research from the University of Plymouth shows that out of a sample of 400 teachers, 31 per cent had experienced online abuse from both pupils and parents.

Social media can also create additional criminal activity. Furthermore, approximately 350 inmates were found to be using Facebook to communicate with the outside world through smartphones smuggled into the prison. This allowed some to continue orchestrating criminal activity from inside the confines of the prison.[64] In November 2012, the Justice Secretary also announced a crackdown on the use of social media by criminals to intimidate and terrorise witnesses.[65]

The amount of personal information posted on social media increases individuals' risk of burglary. UK home security experts Friedland, found that, when interviewed, 78 per cent of ex-burglars said that they strongly believed that social media platforms are being used by thieves when targeting property. Similar research found that many burglars undertook significant research before targeting a house, and social media can provide a gold mine of information, with people unwittingly publishing addresses and full details of where they are and when they are away.[66]

Jurisdiction

There is a wide and well known difficulty with jurisdiction. There have been increasing efforts by governments to regulate content more generally – usually by asking or encouraging ISPs to take more responsibility over the content that they make available online. But regulating content is fraught with legal and practical difficulties.

Indeed, it is not clear how to determine under whose legal jurisdiction content falls. One recent debate – as yet unresolved – is whether Cloud content is subject to the US Patriot Act, because it is mainly held on US servers (even if the producer of that content might be based outside the US). Indeed, different EU rulings appear to have considered these issues irrelevant if they affect an EU Citizen – wherever they are hosted. This is potentially a major problem as every piece of content could be subject to every (separate) national law.[67]

Generally speaking, if ISPs are aware of illegal content hosted on their site, they are asked to remove it, and usually comply. According to the European E-Commerce directive, ISPs are responsible for content they host or provide access to: 'If an ISP is acting as a host of information, it will not be liable for information provided that it does not know that the information is illegal and acts expeditiously to remove or to disable access to information.' However, one of the crucial questions regarding ISP liability is what will constitute 'knowledge' of illegal content, and what 'act expeditiously' means.[68]

In addition to these legal and jurisdictional problems, practical problems can complicate matters still further. The viral nature of online hate makes legal policing an unrealistic challenge, except in cases where authorities want to 'set an example.'[69] Indeed, anonymity online is also problematic, since it permits the author of offensive comments to avoid being penalized for his or her actions.[70] Moreover, heavy regulation may be effective in terms of impacting the major social networks, and high-volume websites in the 'open' internet, but probably the most radical, hateful and problematic discussions occur in closed forums, or the dark web through TOR portals – which are harder or impossible to regulate. As such, some analysts have argued that criminal justice agencies have been limited in their willingness to investigate offences that are not a significant public priority.[71]

Use, storage and disposal

In so far as they are used for policing purposes, data from social media is regulated by the Code of Practice on the Management of Police Information (MOPI)[72], which was issued in 2005. Advice on its implementation by forces is given in the guidance, the second edition of which was published in 2010[73], following the judgment of the ECHR on the retention of DNA records in the case of *S and Marper v United Kingdom*.

The code and the guidance set use, storage and disposal in the context of the Data Protection Act, the Human Rights Act and other legislation, while advising on the proper management of the

exceptions which those provisions make for law enforcement. The aim is to balance the requirements for better use of information, especially its aggregation and analysis for intelligence and investigation, with the requirements of proportionality and necessity of purpose. The guidance sets a period of six years for reviewing the need for retention.

The code and the guidance were, unsurprisingly, created without envisaging the use of social media as a source of intelligence by the police. The approach to reviewing the need for retention is couched in terms of individual people or groups of individuals and offences. The criteria for retention are largely in terms of the evaluation of the risk from those individuals or the seriousness of the offences. It is not apparent how this regime should be applied to the retention of collections of social media product beyond that which relates to specific individuals who are the subject of investigation. There is likely to be at the very least a problem of volume for reviewers – indeed, the same consideration is likely to apply wherever the police collect so-called big data in order to carry out analysis for predictive purposes. It is important that the police set out some clear guidance on retention purposes, including how, and when, agencies will dispose of social media data that is not required for either intelligence briefings or continuing investigations.

Demos – Licence to Publish

The work (as defined below) is provided under the terms of this licence ('licence'). The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this licence is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this licence. Demos grants you the rights contained herein consideration of your acceptance of such terms and conditions.

1 Definitions

a 'Collective Work' means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this Licence.

b 'Derivative Work' means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this Licence.

c 'Licensor' means the individual or entity that offers the Work under the terms of this Licence.

d 'Original Author' means the individual or entity who created the Work.

e 'Work' means the copyrightable work of authorship offered under the terms of this Licence.

f 'You' means an individual or entity exercising rights under this Licence who has not previously violated the terms of this Licence with respect to the Work, or who has received express permission from Demos to exercise rights under this Licence despite a previous violation.

2 Fair Use Rights

Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3 Licence Grant

Subject to the terms and conditions of this Licence, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:

a to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

b to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works; The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4 Restrictions

The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this Licence, and You must include a copy of, or the Uniform Resource Identifier for, this Licence with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this Licence or the recipients' exercise of the rights granted hereunder. You may not sublicence the Work. You must keep intact all notices that refer to this Licence and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this Licence Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this Licence. If You create a Collective Work, upon notice from any Licencor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.

b You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital filesharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

C If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works, You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer

A By offering the Work for public release under this Licence, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:

i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;

ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.

B except as expressly stated in this licence or otherwise agreed in writing or required by applicable law, the work is licenced on an 'as is' basis, without warranties of any kind, either express or implied including, without limitation, any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability

Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensor be liable to you on any legal theory for any special, incidental, consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensor has been advised of the possibility of such damages.

7 Termination

A This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence, however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.

B Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.

8 Miscellaneous

A Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.

B If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

C No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

D This Licence constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This Licence may not be modified without the mutual written agreement of Demos and You.

NOTES

[1] There are a number of possible ways to classify police social media use. The COMPOSITE project, funded under the EU's FP7 programme identifies nine: Social Media as a Source of Criminal Information; Having a Voice in Social Media; Social Media to Push Information; Social Media to Leverage the Wisdom of the Crowd; Social Media to Interact with the Public; Social Media for Community Policing; Social Media to Show the Human Side of Policing; Social Media to Support Police IT Infrastructure; Social Media for Efficient Policing. Denef et al, *Best Practice in Police Social Media Adaptation*, 2010, http://www.fit.fraunhofer.de/content/dam/fit/de/documents/COMPOSITE-social-media-best-practice.pdf (accessed 28 Feb 2013)

[2] http://www.west-midlands.police.uk/contact-us/social-networks (accessed28 Feb 2013)

[3] Responsibility for granting authorisations varies depending on the nature of the operation and the public authority involved; and there are a certain number of statutory purposes for which this activity can be legitimately done.

[4] Ibid

[5] http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert?view=Binary.

[6] Denef et al, *Best Practice in Police Social Media Adaptation*, 2010, http://www.fit.fraunhofer.de/content/dam/fit/de/documents/COMPOSITE-social-media-best-practice.pdf (accessed 28 Feb 2013)

[7] http://www.whatsinkenilworth.com/2013/01/uk-police-forces-using-social-media.html (accessed 28 Feb 2013)

[8] Engage: Digital and Social Media Engagement', ACPO, http://www.acpo.police.uk/documents/LPpartnerships/2010/20110518per cent20LPPBAper cent20dm_engage_v61.pdf.>. (accessed 28 Feb 2013)

[9] The MyStarBucksIdea campaign is an early example of this kind of initiative: http://www.starbucks.com/coffeehouse/learn-more/my-starbucks-idea (accessed 28 Feb 2013)

[10] http://www.ted.com/talks/ethan_zuckerman.html (accessed 28 Feb 2013)

[11] Engage: Digital and Social Media Engagement', ACPO, http://www.acpo.police.uk/documents/LPpartnerships/2010/20110518per cent20LPPBAper cent20dm_engage_v61.pdf.>. (accessed 28 Feb 2013)

[12] HMIC, *The Rules of Engagement: Report into the August 2011 Disorders*, 2011, p. 32.

[13] Cabinet Office, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, Oct 2010 www.cabinetoffice.gov.uk/sites/default/files/resources/nationalsecurity-strategy.pdf (accessed 28 Feb 2013)

[14] The Gang Resistance and Training (GREAT) programme, introduced by the Phoenix Police Department in 2001, involved police-led sessions incorporated into the school curriculum to promote conflict-resolution skills, cultural sensitivity and demonstrate the negative consequences of gang life. This scheme, despite being competently run and well managed, demonstrated statistically negligible results not sustained over the long term. Ebensen F., Osgood, D.W. (1999), Gang Resista2013)nce Education and Training (G.R.E.A.T): Results from the national evaluation, Journal of Research in Crime and Delinquency 36. Often cited as a success story, Boston's Operation Ceasefire and the Little Village Gang Violence Reduction Project (GVRP) a number of different non-police actors cooperated in the into counseling and occupational advice programmes, and other community engagement projects.

[15] These are: Metropolitan, West Midlands, Greater Manchester, Central Scotland, Northern, Bedfordshire, Suffolk, Lincolnshire, Hertfordshire, Kent, Thames Valley, Wiltshire, West Mercia, South Yorkshire, West Yorkshire, Cleveland, Devon & Cornwall, Avon & Somerset, Cumbria, Northamptonshire, Leicestershire, Hampshire, Northumbria and Staffordshire.

[16] .We used Facebook Ads to calculate these statistics.

[17] We used SimplyMeasured to run this analysis. http://simplymeasured.com/ (accessed 28 Feb 2013)

[18] We used the Fake Follower Check tool from Statuspeople for this analysis http://fakers.statuspeople.com/Fakers/Scores (accessed 28 Feb 2013)
[19] We used a geo-location tool from Followerwonk for this analysis Followerwonk.com (accessed 28 Feb 2013)
[20] This guidance was also submitted to The Leveson Inquiry.
[21] 'Police officers twitter accounts closed', The Guardian, 3rd October 2012, < http://www.guardian.co.uk/uk/2012/oct/03/police-officers-twitter-accounts-closed>. (accessed 28 Feb 2013)
[22] 'Police officers' Twitter accounts closed after watchdog raises concerns', The Guardian, 3rd October 2012, <http://www.guardian.co.uk/uk/2012/oct/03/police-officers-twitter-accounts-closed>. (accessed 14 Mar 2013)
[23] 'Walsall police sergeant probed over alleged misuse of Twitter', Birmingham Mail, 22nd September 2012, 'http://www.birminghammail.co.uk/news/local-news/walsall-police-sergeant-probed-over-4433 (accessed 14 Mar 2013)
[24] http://www.independent.co.uk/news/uk/crime/pcso-instructed-to-cease-tweeting-8194415.html (accessed 14 Mar 2013)
[25] Interview, [anon]
[26] e.g. the guidance notes that 'West Midlands Police recognizes that traditional methods of communicating messages which have been relied on in the past are having less impact and are reaching fewer people. Therefore there is a real need to embrace other growing forms of communication' http://www.levesoninquiry.org.uk/wp-content/uploads/2012/03/Exhibit-West-Midlands-Police-2.pdf (accessed 14 Mar 2013)
[27] Leveson Inquiry Evidence Day 53 afternoon pp 20-21
[28] Vanessa Kortekass (2011) 'Olympics security in focus after London riots', *Financial Times,* 9 August, http://www.ft.com/cms/s/0/8b9fe0ec-c29e-11e0-8cc7-00144feabdc0.html#axzz2M32i3Ybn
[29] National Centre for Policing Excellence (2007) *Introduction to Intelligence Led Policing* (Bedfordshire: National Centre for Policing Excellence).
[30] HMIC (2011), The Rules of Engagement: A Review of the August 2011 Disorders , p. 31.
[31] http://www.facewatchid.co.uk/ (accessed 28 Feb 2013)
[32] See #Intelligence, (Demos, 2012)
[33] Xiang, R, Neville, J, Rogati, (2010) M, *Modelling Relationship Strength in Online Social Networks*, http://snap.stanford.edu/nipsgraphs2009/papers/xiang-paper.pdf (accessed 19 March 2013)
[34] Valenzuela, S, Arriagada, A and Scherman, A, *A trend study of social media and protest behavior: Facebook, Twitter and youth mobilization in Chile (2009-2012)* http://www.academia.edu/2444268/A_trend_study_of_social_media_and_protest_behavior_Facebook_Twitter_and_youth_mobilization_in_Chile_2009-2012_ (accessed 19 March 2013)
[35] Sakaki, T, (2010) *Earthquake Shakes Twitter Users: Real-time Event Detection by Social Sensors,* University of Tokoyo.
[36] http://www.whatdotheyknow.com/request/social_media_monitoring_policies#incoming-250931 (accessed 19 March 2013)
[37] http://www.whatdotheyknow.com/request/social_media_monitoring_policies_2# (accessed 19 March 2013)
[38] http://www.bigbrotherwatch.org.uk/home/2011/09/westminster-council-unveils-plans-for-social-media-monitoring.html (accessed 19 March 2013)
[39] See #Intelligence (Demos, 2012)
[40] Suler, J. (2004). CyberPsychology and Behavior, 7, 321-326 http://users.rider.edu/~suler/psycyber/disinhibit.html (accessed 19 March 2013)
[41] Eaton, E. (2012). There are more 'Fake' People on Facebook than Real Ones on Instagram. *Fast Company*
[42] See, for example, the social media persona 'Shooter Kirpachi' which was infiltrated several Islamist sites.

[43] Syria Gay Girl in Damascus Blog a Hoax by a US man. (2011). *BBC News*. http://www.bbc.co.uk/news/world-middle-east-13744980 (accessed 14 Mar 2013)
[44] Liu, B., Mukherjee, A. & Glance, N. (2012). Spotting Fake Reviewer Groups in Consumer Reviews. *International World Wide Web Conference Committee.* http://www.cs.uic.edu/~liub/publications/WWW-2012-group-spam-camera-final.pdf (accessed 14 Mar 2013)
[45] Streitfeld, D. (2012). The Best Book Reviews Money Can Buy. *The New York Times.* http://www.nytimes.com/2012/08/26/business/book-reviewers-for-hire-meet-a-demand-for-online-raves.html (accessed 20 March 2013)
[46] Depending on the type of intrusion, the authorising officer could be a police superintendent or even the Home Secretary when intercept methods are proposed.
[47] There are five codes of practice of the different intelligence collection set out under RIPA (interception of communications, acquisition and disclosure of communications data, covert surveillance and property interference, covert human intelligence sources, investigation of protected electronic communication. We believe that SOCMINT is most likely to fall under the following: covert/directed surveillance, interception of communications, and covert human intelligence sources. We therefore limit our discussion to these parts. Property interference (often known as 'intrusive covert surveillance' may be applicable in respect of closed profile pages).
[48] http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert?view=Binary (accessed 20 March 2013)
[49] Covert surveillance covers 'intrusive surveillance' which takes place in residential premises or a private vehicle, or 'directed surveillance' which is not intrusive but is likely to result in the obtaining of private information.
[50] Principally: in the interests of national security; for the purposes of preventing or detecting serious crime; and for the purpose of safeguarding the economic well being of the UK.
[51] 'DPP statement on Tom Daley case and social media prosecutions', CPS Blog, 20th September 2012, http://blog.cps.gov.uk/2012/09/dpp-statement-on-tom-daley-case-and-social-media-prosecutions.html (accessed 20 March 2013)
[52] http://cdn.weinterrupt.com/wp-content/uploads/images-17.jpg (accessed 20 March 2013)
[53]http://www.journal-online.co.uk/article/5410-police-use-facebook-to-identify-weapon-carriers (accessed 20 March 2013)
[54] Public Safety Canada (2011) *Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities*,
[55] http://www.lyonsdavidson.co.uk/news/1051/facebook-evidence-a-defendant-solicitors-view (accesed 20 March 2013)
[56] Zelin, A, (2013) The State of Global Jihad online, New America Foundation
[57] http://www.independent.co.uk/news/uk/crime/activists-warned-to-watch-what-they-say-as-social-media-monitoring-becomes-next-big-thing-in-law-enforcement-8191977.html (accessed 20 March 2013)
[58] http://www.digitaltrends.com/social-media/nypd-create-unit-to-track-criminals-on-social-networks/ (accessed 20 March 2013)
[59] http://www.reuters.com/article/2012/02/07/us-germany-facebook-idUSTRE8161LG20120207?feedType=RSS&per cent3BfeedName=internetNews (accessed 20 March 2013)

[60] Interview, anonymous
[61] Google Transparency Report: United Kingdom 2012 https://www.google.com/transparencyreport/removals/government/GB/ (accessed 20 March 2013)
[62] http://www.telegraph.co.uk/technology/facebook/9323700/Trolling-abuse-got-worse-for-victim-Nicola-Brookes-after-Facebook-victory.html (accessed 20 March 2013)

[63] http://metro.co.uk/2010/05/22/facebook-bullies-believed-to-have-caused-teenagers-suicide-324409/ (accessed 20 March 2013)
[64] http://www.dailymail.co.uk/news/article-2154624/A-Facebook-crime-40-minutes-12-300-cases-linked-site.html (accessed 20 March 2013)
[65] http://www.standard.co.uk/news/crime/justice-secretary-well-stop-convicts-using-social-media-for-threats-8335511.html (accessed 20 March 2013)
[66] http://www.telegraph.co.uk/technology/facebook/7900704/Burglars-using-Twitter-and-Facebook-to-case-the-joint.html (accessed 20 March 2013)
[67] Goldsmith, J and Wu, T, *Who Controls the Internet?* (CUP, 2006).
[68] Vanacker, B, *Global Medium - Local Laws*, El Paso: LFB Scholarly Pub., 2009.
[69] Wolf, C, 'The Role of The Internet Community in Combating Hate Speech', Berin Szoka and Adam Marcus (eds) *The Next Digital Decade: Essays on the Future of the Internet*, TechFreedom: Washington, D.C., 2010 http://nextdigitaldecade.com/ndd_book.pdf (accessed 20 March 2013)
[70] Levmore, S, 'The internet's anonymity problem' in Saul Levmore and Martha. C. Nussbaum (eds.) *The Offensive Internet – Speech, Privacy, and Reputation*, Harvard University Press: Cambridge, 2010, pp. 50-67.
[71] James Banks, *European Regulation of Cross-Border Hate Speech in Cyberspace: The Limits of Legislation*, European Journal of Crime, Criminal Law and Criminal Justice, 2011, 19:1-13, http://shu.academia.edu/JamesBanks/Papers/1050646/Banks_J._2011_European_Regulation_of_Cross-Border_Hate_Speech_in_Cyberspace_The_Limits_of_Legislation_European_Journal_of_Crime_Criminal_Law_and_Criminal_Justice_19_1-13 (accessed 19 March 2013)
[72] http://www.cleveland.police.uk/downloads/Code_of_Practice_on_MoPI.pdf (accessed 19 March 2013)
[73] http://www.acpo.police.uk/documents/information/2010/201004INFMOPI01.pdf (accessed 19 March 2013)