

Online Social Networking, Order and Disorder

Russell Lock, Louise Cooke and Tom Jackson
Loughborough University, Loughborough, UK
r.lock@lboro.ac.uk

Abstract: Whilst online social networking has been used successfully for many years by all strata of the world's population, its use to ferment and prevent civil disturbances is a relatively new phenomenon. It is clear that the way in which online social networking sites are being used is evolving, and that changing user perceptions of online privacy may impact on the ability of the law enforcement community to adapt to new methods of monitoring and evidence gathering. This paper focuses primarily on the London riots of August 2011, and as such discusses legal issues from a UK perspective. However, the matters discussed are of relevance worldwide, with reference made to similar events outside the UK, to show that what occurred in London was not an isolated incident, or a quirk of the UK social networking scene. This paper explores what occurred, the platforms that were used and how they were used, and the legal framework in which investigations took place. It examines the use of social networking to organise rioters, support community defence, and shape the response of law enforcement agencies such as the police, government and the courts. It concludes that there is significant potential for problems of this type to occur in the future, which will require the evolution of law enforcement methods and procedures, and could change the way in which the law enforcement community utilise e-Government systems.

Keywords: Social Networking, Law Enforcement, London Riots, Future Trends

1 Introduction

Online Social Networking Sites (SNS) have become a pervasive element of society. However, policing their use remains a significant problem for law enforcement agencies. Such agencies frequently have to apply laws which are outdated, and struggle to apply conventional resources such as the UK Criminal Justice and Public Order Act 1994 (UK Government 1994), to problems that require new techniques for the efficient gathering and analysis of online evidence. The events that took place in August 2011 in London and other UK cities showed that social networking could be a force for public order or disorder. They highlighted the attempts of government to handle new threats, the police to deal with a considerable ongoing influx of electronic evidence, much of it submitted directly by the public, and by the courts to handle operation 24 hours a day to cope with the number of cases. This paper examines the current state of online SNS with regard to civil disturbances, using the London riots as a case study. The paper is therefore UK-centric in terms of law, but highlights global problems.

The structure of the paper is as follows. The remainder of this section outlines the context to the riots that occurred during August 2011, and provides perspective on the scale of events. Section 2 explores background research relevant to the domain in question, focussing on internet controls, end user actions to support the law enforcement community, and specific platform capabilities. Section 3 discusses the way in which flash mobs are facilitated by online SNS, using data gathered from social networks during the London riots. Section 3 also looks at the support the UK's current legal framework provides to the law enforcement community for handling civil disturbances exacerbated by online SNS. Section 4 examines the direction in which online SNS are evolving with reference to the potential for future problems of this type. Finally, section 5 discusses the potential for future research within the area and provides conclusions.

1.1 Context of the riots

The majority of the activity associated with the London riots occurred between the 6th and 17th August 2011. Initially confined to London, disturbances spread to a number of other cities in the UK including, Birmingham, Liverpool, Manchester and Nottingham. For the purposes of this paper the term 'London riots' will cover events both within and outside London, as this was the term used by the media at that time. Although many viewed the riots as without justification (that looting was the main purpose), it is clear that there was a flashpoint incident which contributed to the first riot in Tottenham London on the 6th August. The incident concerned Mark Duggan, who was shot and killed during his arrest by CO19 (the London police force's specialist firearms unit) on the 4th August. The shooting led to an initially peaceful protest march, organised by the family of the deceased on the 6th August. The march attracted undesirable elements who became more violent as time passed, leading to large scale rioting overnight within the London suburb of Tottenham. Over

the following days rioting spread to other London suburbs including Hackney. Rioting also spread to other cities, even as disturbances within London itself subsided.

1.2 The scale of the riots

The following facts were taken from the Metropolitan Police Service force's strategic review (Metropolitan Police Service 2011) into the riots, unless otherwise stated.

- The cost of the riots to insurance companies has been placed at around £250million
- The cost of the Metropolitan Police Service operations within London to be in excess of £34 million.

Five people were killed, three in a single hit and run incident whilst the victims were attempting to defend property in Birmingham.

Approximately 2100 people were charged for approximately 3200 separate offences, with ages ranging from an 11 year old charged for stealing a bin (Somaiya 2011), to a 70 year old arrested for looting a branch of Sainsbury's (The Mirror 2011).

1.3 Data collection method

The sources used within this paper include government and law enforcement statements, delivered either through official channels or released to the media and SNS data. Media reporting contains significant potential for bias, and as such has only been used to report facts relating to legal cases (where official sources have not yet published their data), or to illustrate the nature of the reporting by the media of the riots.

Where possible the information included within the paper has been verified through multiple sources. In the case of media articles the authors accept that a lack of independence between articles formed on secondary evidence may lead to a false measure of accuracy.

The Twitter dataset analysed within the paper was gathered using third party social network data mining tools due to Twitter's limited inbuilt search functionality, and was gathered retrospectively in the months that followed the riots. It is therefore possible that tweets may have been removed in the intervening period between publishing and retrieval, a phenomenon which was indirectly observable for some online SNS during the period including Flickr.

2 Background

Many research areas have a bearing on the study of online SNS when considering their support for rioters, community defence and law enforcement. This section focuses on four key areas, those of government control of the internet in a global context; the perception of privacy engendered within the community of online SNS users; the willingness of the public to use the internet to support law enforcement processes; and finally the communication facilities common online SNS provide to rioters, community defence and the law enforcement community.

The monitoring of SNS by members of the public and the authorities can take two distinct forms, those of horizontal and vertical surveillance (Sewell 1998). Regulatory approaches such as laws are applied vertically from the top down upon all internet users, whereas official (by the police for example) or unofficial (by users) surveillance of individuals and groups forms horizontal surveillance. The concept of horizontal surveillance is common within societies, with one of its most obvious applications being that of peer pressure to conform to a perceived ideal. The relative lack of effective, organised vertical and horizontal surveillance of SNS enables dissident groups to flourish by reducing the risks of discovery and prosecution, in-line with existing thinking on social exchange theory (Emerson 1976).

In a study by Obar (Obar, Zube & Lampe 2012) research into advocacy groups within the USA found that out of 53 groups surveyed, 98% of them used Facebook, 96% Twitter and 77% YouTube. The study focussed on established advocacy groups rather than the more temporary alliances observed during the London Riots. Obar's research findings identified links between participation and information technology literacy gaps based on generation, however the research did not extend to quantifying the extent to which this affected the

advocacy groups, or to explore the rate of change over time. The study also identified a higher proportion of female participants, a point reinforced by numerous studies on SNS, including Tokunaga (Tokunaga 2011).

In related research, Nisbet (Nisbet 2008) highlighted the role of mass media in encouraging convergence of viewpoint on issues. Shanahan (Shanahan, Morgan 1999) reported that the effect of media on dissident groups exhibited a stronger convergence effect than on others. Nisbet stressed the need for control structures to underpin the role of media as a regulating force in democracies. Considerable research still needs to be completed in this area to determine if online behaviour and offline behaviour can be examined using the same theories. However, it is clear that the lack of societal oversight caused by privacy settings on groups, posts etc would have the effect of weakening control mechanisms, making self regulation within communities more common. Where those communities are dissident in nature the effect of self regulation is likely to be reduced by the bias introduced to the community.

2.1 Government intervention on the internet

Government control over online SNS differs significantly around the world. A number of countries restrict access to either specific SNS accounts/pages or entire platforms in order to prevent perceived dissident use. These countries currently include Bahrain, Belarus, Burma, China, Cuba, Ethiopia, Iran, Kazakhstan, Pakistan, Saudi Arabia, South Korea, Thailand, Tunisia, Turkey and Vietnam (Kelly, Cook 2011). Iran in particular has been criticised for its threats against Iranians outside the country who are disenchanted with the current government, in some cases leading to detainment and arrest (Fassahi 2009)(Erdbrink 2012). The UK currently occupies 5th place in the Internet Freedom report (Kelly, Cook 2011), but appears to be on a gradual downward trajectory. It is arguable that the use of tools such as Facebook during the Arab Spring of 2011 is likely to increase censorship around the world in future years, and that any changes to the law following the London riots may impact negatively on the score the UK receives in future.

The reaction of world governments to civil unrest has in the past extended to the blocking of social networking and/or web access, restricting the dissemination of information by the public. This seems an extreme measure however, as blocking access also deprives authorities of the intelligence that social networking can provide.

Within the UK, in addition to the legal framework, a process exists to monitor and block some web materials, however it is not government controlled. The Internet Service Providers Association (ISPA), a trade association for Internet Service Providers (ISPs), has implemented self-regulation by adhering to requests made by the Internet Watch Foundation (IWF), a charity, on what internet material should be blocked within the UK. To date, the powers of the IWF have been limited to blocking sites hosting content that is illegal under UK law, such as child pornography and racial hatred. Such blocks are achieved using content filtering software such as Cleanfeed.

2.2 User perceptions of social networking privacy

There is a considerable body of evidence which suggests that the ubiquity of membership to online SNS, particularly among younger people, is changing popular attitudes towards personal privacy. Gross (Gross, Acquisti & Heinz III 2005) analysed the privacy preferences of more than 40,000 US students using online SNS, and found that only a minimal proportion changed their preferences from the default open settings. During the London riots a number of arrests were made based on information publicly shared on sites such as Facebook (The Crown Prosecution Service 2011). Fogel and Nehmad (Fogel, Nehmad 2009) also studied the attitude of college students towards privacy, trust and risk-taking on online SNS, and found that those who had profiles on the sites expressed higher levels of trust, and were more open to risk-taking than those who did not. Paradoxically, in an empirical study of young Australian users, Robards' research (Robards 2010) concluded that young people increasingly regard social network sites as private spaces to 'hang out', akin to teenagers' bedrooms, or to shopping centres and parks. He goes on to argue that, across the world, young people are developing ever more complex strategies to protect and preserve their privacy online. These contrasting findings highlight the difficult and complex nature of changing and diverse user attitudes towards privacy, and the double-edged nature of social networking via the internet as a tool either for the co-ordination of protest and civil disorder, or to advance criminal investigation into such disorder.

The vast amount of user submitted data, accumulating at an estimated 30 billion (US) pieces per month for Facebook alone (Facebook 2011), is of considerable value to the law enforcement community. However,

leveraging such information also has the potential to form a digital panopticon, where civil liberties are suppressed by ongoing monitoring and analysis.

2.3 Public support for online law enforcement activities

There have been numerous instances of the general public making use of online SNS to retrieve stolen goods, including an incident during the London riots (BBC News 2011a). In this instance the owner used remote access software to determine the criminal's personal details from their web browsing habits. The criminal's Facebook page provided sufficient information for the police to find and arrest the individual. It is worth noting that the inverse case also holds, that if a criminal can access an individual's Facebook profile they may be able to determine where that person lives, whether they are currently on holiday and have left their property unguarded etc.,. Cases of identity theft using social network data are also becoming more common, and are an active area of academic research (Bilge et al. 2009, Nosko, Wood & Molema 2010).

The active participation of victims in the investigation of theft involving internet enabled devices such as phones and laptops is becoming more commonplace, as both free and commercial tools are available to support the locating of such devices including LocateMe¹ and Find My iPhone². The UK Police endorse the Immobilise³ possession ownership database, a free third party service that allows the police to match seized property with its original owners. This service complements existing government sponsored services such as the NMPR (National Mobile Property Register)⁴, and third party purchase investigation services such as CheckMEND⁵. It is arguable that given the limited resources of the police, both the free and commercial sector may provide useful capabilities to complement those of the police.

2.4 Social networking platform capabilities

The London riots involved considerable use of online SNS. The following section explores the capabilities of four major platforms that were associated with communication during the riots.

BBM (BlackBerry Messenger)

BBM is an instant messenger platform that allows one-to-one and group messaging. In its simplest form it is similar to SMS, but with unrestricted message length. BBM also supports picture messaging, geotagging etc. A number of countries, including India and UAE, have threatened to block the use of BBM given the relative privacy it offers to its clients. Surveillance on BBM by the police without the cooperation of RIM Ltd (Research in Motion) is currently infeasible on a large scale due to resource limitations, given that encryption is used to secure messages.

Facebook

Facebook lends itself to the organisation of events through public pages (where anyone can view a message) or private pages (where only those invited can view the page). In addition to this, a private page can be secret (groups cannot be found in searches and non-members cannot see anything about the group). Once the security of a page has been determined, there are many ways to communicate with the group. One relatively recent innovation, Facebook Messenger, provides a stand-alone mobile application that enables messaging directly to group members' phones. The relative privacy of online groups is a potential issue for law enforcement agencies.

Twitter

Although Twitter was used maliciously during the riots it is not the strongest platform for this particular type of application. Twitter allows people to broadcast short (140 character) statements to the world, or to their closed group of followers. Twitter was not conceived with two way communication in mind, though it does support it with three mechanisms:

¹ LocateMe <http://code.google.com/p/locateme/> consulted 5/9/2011

² Find My iPhone <http://www.apple.com/uk/iphone/features/find-my-iphone.html> consulted 19/9/2011

³ Immobilise <http://www.immobilise.com/about.html> consulted 6/9/2011

⁴ NMPR <http://thenmpr.com/> consulted 21/3/2012

⁵ CheckMEND <http://www.checkmend.com/uk/> consulted 21/3/2012

- A private message can be sent to another person, subject to the character limit, however such limited point to point communications are not ideal to organise large groups.
- Replies can be posted to a specific statement using an @ hashtag
- Using the # hashtag, a statement can be made which is easier for non followers to search for using Twitter's trending feature. However, for a large scale incident any given message is unlikely to make much impact (given the number of postings).

One of the limitations for criminal use of Twitter is its limited privacy functions. Although it is possible to make a Twitter feed private, any person who follows it could make a reference to it using the @ hashtag on their own potentially public feed, effectively providing clues to the law enforcement community on what statements have been made on the private feed.

YouTube

YouTube was not originally conceived as a SNS (Boyd, Ellison 2007), however given its current features include, messaging, trending and commenting it could now be considered one. Videos uploaded are predominantly public in nature, though YouTube does have the facility for private video hosting. YouTube is not ideally suited to private communications, as private videos have an access control limitation of 50 viewers. Therefore in terms of communication relating to civil disturbance the ability to privately discuss and plan using the platform is limited.

3 The London Riots in context

In order to explore the way in which online SNS impacted on the London riots it is first necessary to understand the much older concept of flash mobs, to which an introduction is provided in section 3.1. Section 3 then builds upon this by exploring the way in which online SNS were observed to impact on the London riots, before finally discussing the support the current UK legal framework provides in dealing with the monitoring, handling and evidence gathering associated with this type of disturbance.

3.1 Flash Mobs

Dependent on the context, Flash Mobs, where groups of individuals arrange in advance to meet up at a specific time and place, can be either a force for order or public disorder. Dating back to the early 2000s, Flash Mobs were primarily conceived as an art form. One author described them as instances of 'tactical frivolity' (Amparo, Martínez de Albéniz 2009)

One of the earliest recognised flash mobs involved 300 people converging on Toys "R" Us in Time Square New York, and spontaneously worshipping at the feet of a large dinosaur, before peacefully dispersing a few minutes later (Cayley 2009). The related term Smart Mob may also be encountered, though media sources rarely use the term, to describe longer term activities with specific goals, often political such as those associated with the Arab Spring of 2011.

Although arguably not the most accurate source of information it is interesting to note from a societal perspective that Wikipedia's definition of Flash Mobs (Wikipedia 2011) was modified to include the potential use of violence, around the time of the London riots of 2011. However, the dictionary definitions quoted in support of the article still show the pre-2011 concept of flash mobs as 'pointless activities'⁶ (as of the 23rd August 2011). It would appear the events of 2011 are outpacing the definition of how such concepts can be used. The pace of evolution may cause difficulties in applying current legal frameworks, something which may be evident in the variety of sentences given for similar crimes during the period in question.

3.2 Online SNS, Rioters, Community and the law

Amparo and Martinez de Albeniz (Amparo, Martínez de Albéniz 2009) were early believers that the definition of a Flash Mob should encompass the potential for political and violent behaviour, proposing that the main utility of Social Networking and mobile devices in support of such behaviour includes:

⁶ Defined as "a public gathering of complete strangers, organized via the Internet or mobile phone, who perform a pointless act and then disperse again." Oxford Dictionaries, Published by the Oxford University Press. <http://oxforddictionaries.com/> consulted 6/9/2011

- Calls to mobilisation (to demonstrations, protests, violence etc)
- As a communication platform for activities
- For the dissemination of news, rumour and propaganda
- To support citizen surveillance activities
- The use of technology to support technological activism such as hacking (sometimes referred to as hacktivism⁷)
- To chronicle the activities undertaken for a particular cause.

The use of social networking for protest purposes has varied from small scale activities to large scale protest groups such as the No Mas Farc group in Columbia, which had 13 million Facebook followers (Etling, Faris & Palfrey 2010) (Laer, Aelst 2009) at its peak. One notable phenomenon seen in these cases appears to be a belief in safety in numbers. It is plausible that many of those who have subsequently been charged for offences relating to social networking during the London riots believed the same thing. Laer (ibid) separated the actions taken by citizens into 'internet based' and 'internet supported' in order to separate those activities that were designed to enhance existing physical activities through technology, such as organising a demonstration, from those that use technology to achieve something purely virtual such as hacking, the creation of protest websites etc. Laer further postulated that the internet had lowered the thresholds associated with undertaking such activities, i.e. that the internet has made it considerably easier for people to perform acts of civil disobedience. Consider the options open to a protestor in the 1980s who wished to spread a message, compared to that of a protestor today. What would have entailed a significant amount of time and resources in spreading a message via perhaps volunteers and pamphlets can now be achieved virtually using Twitter, in a matter of seconds.

However, the public backlash against such online actions can be equally swift. A number of examples (BBC News 2011c) were recorded during the London riots of citizens reporting social networking pages/feeds that were involved in illegal activities. Citizens were also quick to place a petition on the number 10 Downing Street petition page to strip offenders of social housing if they received it (247,364 signatories as of 5th October 2011); a movement so popular it overloaded the petition system for several hours (BBC News 2011b). Perhaps more ominously Laer also discusses transnational characteristics of social networking. Given the global recession in 2011 were they fortunate that the seemingly purposeless rioting did not cross national boundaries?

Two of the more unanticipated uses of social media during the riots were as a force for community defence and cleanup activities. The Twitter feed @riotcleanup attracted over 74,000 followers (as of 19/9/2011), the #Londonriots trending tag was also used extensively (over 55,700 times as of 22/3/2013). Facebook groups such as Liverpool Cleanup, which has 849 members⁸ helped organise community cleanup events in the wake of the riots. Some groups including 'Singhs Defending Southall Gurdwaras'⁹ used social networking sites such as Facebook to organise themselves during the riots to defend property. The police response to what could be termed vigilante behaviour by some groups was muted, possibly due to the number of cases involved in the riots, and overstretched police resources during the riots, which left many areas temporarily un-defendable by traditional means.

One of the most useful aspects of Facebook within the law enforcement community is the relationships it highlights between individuals. Mcillwain (Mcillwain 1999) postulated that 'upperworld' and 'underworld' actors are bound into "social systems of organized crime". Such relationships are undoubtedly one of the more useful features from the perspectives of investigation and evidence gathering. However, social networks such as Facebook and Twitter provide only a binary relationship of friend/follower or not friend/follower (Livingstone 2008). It is also notable that definition for behaviour need to go beyond that of the traditional view of organised crime outlined by Mcillwain, to encompass the more casual, opportunistic and spontaneous elements evident during the London riots.

⁷ Defined as "a person who attempts to gain unauthorized access to computer files or networks to further social or political ends" Oxford Dictionaries, Published by the Oxford University Press. <http://oxforddictionaries.com/> consulted 6/9/2011

⁸ <http://www.facebook.com/event.php?eid=158783327533310> consulted 19/9/2011

⁹ <http://www.facebook.com/pages/Singhs-Defending-Southall-Gurdwaras-UKLondon-Riots/249763281710657> consulted 19/9/2011

3.3 The online presence of the Metropolitan Police Service

The following section examines the ways in which SNS are used by the Metropolitan Police Service (the main police body within the greater London area). It focuses on two key communication platforms, Twitter and YouTube. The section does not cover Facebook, as the Metropolitan Police Service Facebook page was created in response to the London Riots (December 2011), however they now make extensive use of Facebook to elaborate on the initiatives outlined in their Twitter feed.

3.3.1 Twitter

The Metropolitan Police Service operates multiple Twitter feeds, including sub-feeds for each London Borough police force (created after the riots), however their primary Twitter feed for outgoing messages is @metpoliceuk. Figure 1 illustrates the increase in official tweets by the Metropolitan Police Service during the riot period. The red line indicates the average number of tweets per day since the account was created (to 22/3/2013), as approximately 6 per day, rising to 16 per day during the main period of riots and subsequent arrests. Research by Krishnamurphy et al (Krishnamurphy, Gill & Arlitt 2008) defined three broad categories for Twitter users:

- Broadcasters (Who have large followings without reciprocating)
- Acquaintances (With similar numbers of those following and followers)
- Spammers, Evangelists (Who follow without reciprocation)

By this categorisation the @metpoliceuk feed is a broadcaster. The same is true of the London Borough Twitter sub-feeds.

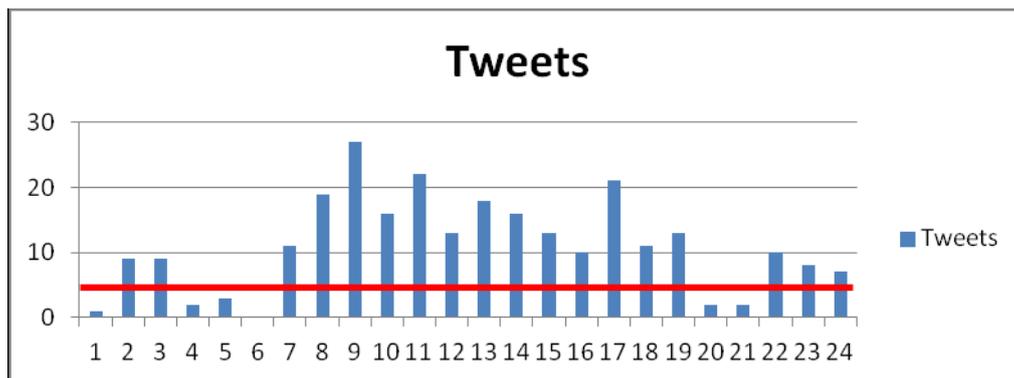


Figure 1: Twitter use by the Metropolitan Police Service

The scope of the current research did not extend to in-depth analysis of the messages sent, however, the following key points were noted:

- A decision was made to move from individual crime reporting to the reporting of aggregate crime figures for the riot period. These tweets focussed on tallies on the number of incidents and associated arrest figures.
- The police did not make use of the #londonriots trending tag. This had two particularly notable effects:
- The popularity of the #londonriots tag could not directly increase viewing of the Metropolitan Police Service Twitter feed via Twitter's trending function.
- Consequently, this allowed the Metropolitan Police Service to avoid using the term 'londonriots' in public communications.

The police made extensive use of Flickr, posting pages of CCTV images via Twitter to engage the public in identifying criminal behaviour (these images have since been removed from Flickr, though they do make use of Flickr to identify suspects and stolen goods for many offences).

It is also worth noting that a report by a police officer within the London Metropolitan Police Service prior to the first night of the riots was raised in their strategic review (Metropolitan Police Service 2011). In the incident an officer reported reading three identical Tweets on separate feeds "Hearing there's a riot in Tottenham you know or they planning one. I hope this is the start of a new era and people start deading feds".

The Metropolitan Police Service investigated that afternoon, but did not believe there was cause for concern. The strategic review believed this was not a failing of intelligence, given the incidents that occurred were unprecedented for London. The strategic review recommended considerably more effort be placed into infrastructure and resourcing for social networking going forward, of which the new Facebook presence, and sub-Twitter feeds played a prominent role.

3.3.2 YouTube

The Metropolitan Police Service YouTube channel is used predominantly to give advice on crime prevention, to explain police procedures, and occasionally to show CCTV footage relating to cases. However, despite averaging approx 6 videos per month during the period 2012-2013 it was not used for communication during the London riots (given Flickr was used temporarily, but the images were later removed; it is possible the same was true of YouTube). The strategic review (Metropolitan Police Service 2011) categorised the Metropolitan Police Service use of Youtube as 'sporadic' and primarily for 'one way dialogue'.

Youtube was however used extensively by others to communicate and comment upon the incidents that took place. In many instances this involved footage illegally recorded from news channels, which highlights the issues YouTube has in policing itself.

3.4 Online Crime reporting by the public

This section predominantly examines the role that online presence plays in crime reporting within London, however, considerable research could usefully be undertaken to explore the wider use of social media by the 43 separate police forces within the UK.

Crimes relating to internet fraud do have a centralised web point of contact within the UK (ActionFraud.police.uk), however this is run by the National Fraud Authority rather than the police directly, and therefore has a relatively narrow remit for reporting. The process of reporting is questionnaire based, lacking the immediacy of many forms of social media. Within London Metropolitan Police Service PCeU (Police Central e-Crime Unit) operates across a wider remit allowing the reporting of offline crimes online, however the process is again relatively bureaucratic in terms of the information required to report, for example, a crime being planned through a social networking page. The website¹⁰ also sets a relatively poor standard for WCAG¹¹ compliance by little or no guidance for filling in the online forms. This is a significant issue when considering the geographic placement of a given crime. Take the following scenario:

A person observes a crime being planned by a third party using a social networking site.

The PCeU website will only investigate crimes in the Greater London area. Does this therefore imply that in order to use the service:

- A) The observer be London based?
- B) The criminal be London based?
- C) The webserver be London based? (which is likely to be implausible for the observer to determine)
- D) The crime that is being planned should take place in London?
- E) All, some, or none of the above?

Interestingly, the Metropolitan Police Service force Facebook page states explicitly that crimes should not be reported to them via it. Further, as the page states that content on their page is not monitored 24 hours a day, the only way to report inappropriate behaviour on their page is via email. They make very clear that crimes observed online should be reported by phone only (via 999 or 101).

The same statement is made on their Twitter feed, however, despite the clarity of the message many people choose to ignore this. During a one day snapshot (24/3/2013) of @metpoliceuk the following data were collected:

- Mentions: 56

¹⁰ Metropolitan Police Service reporting <https://online.met.police.uk/report/report.php> Accessed 25/3/2013

¹¹ W3C WCAG 2.0 Standard <http://www.w3.org/TR/WCAG/> Accessed 25/3/2013

- Mentions attempting to report crimes: 9
- Percentage: 16%

Many of the messages related to minor road traffic crimes, and had associated images uploaded. This indicates that although the police do not wish to receive crime reports in this manner, it is arguable that the current online system is considered too cumbersome to report minor infractions identified by the public, or that many are not aware of its role.

The Metropolitan Police Service YouTube channel goes one step further by stating that messages sent to them via the YouTube message service are not read, highlighting an issue relating to the extent to which SNS can be customised to their users needs.

3.5 Legal support for online police activities

Organisations such as Facebook, RIM (Research in Motion) and Twitter were quick to state support for the law enforcement community. However, a number of instances have been reported in the past of less than adequate support, including those by Milivojevic (Milivojevic 2011)

"The Australian Federal Police (AFP) Assistant Commissioner and Head of High Tech Crime Operations, Neil Gaughan, is quoted as saying that 'Facebook's woeful relationship with law enforcement bodies is hampering police investigation and putting lives at risk'"

Time Magazine (Handley 2010) featured an article in 2010 discussing British Government issues relating to the removal of the Facebook content of known criminals. The article includes a prominent quote by Richard Allan, director of policy for Facebook within Europe:

"We have 400 million active users and a tiny, tiny staff. We need to find novel ways to handle that kind of crushing amount of activity. It's the burden of being so immensely popular."

Given the recent disturbances in London companies such as Facebook are likely to have to adapt their procedures, as are the police (May 2011). One suggestion raised during the riots was that in future the British government should be able to block access to SNS in times of civil unrest. During the riots there had been some calls to shut down the Blackberry messenger service given its role in riot organisation (Pettifor, Gregory & Layton 2011). Such a decision within a democratic country is not unprecedented. On the 11th of August 2011, the San Francisco BART (Bay Area Rapid Transit) network blocked access to mobile phones within their stations, in order to forestall a protest rumoured to take place that day, prompting an FCC investigation (The Federal Communications Commission 2012).

In terms of deterring crime, some of the longer sentences given to rioters related to incitement to riot via social networking sites, including the four year sentences given to Jordan Blackshaw and Sutcliffe Keenan (The Crown Prosecution Service 2011), despite the disturbances they planned not having occurred. Their subsequent appeal against what their lawyer termed 'manifestly unfair' sentencing was rejected. This opens an interesting debate on the meaning of data stored across social networking sites. Without visual and audio cues to provide additional insight and context for a given action, police only have the posted written statements from which to derive meaning. The ongoing publication of aspects of our lives using social media, without consideration for how such information may be received by law authorities, employers, friends and strangers was dubbed "communicating in their [sic] virtual underwear" in one notable publication (Rosenblum 2007). There have been a considerable number of court cases where evidence from social networking has either been used in order to indict, or has involved dubious or unacceptable conduct on the behalf of jurors, lawyers and even judges (Nelson, Simek & Foltin 2009). In one court case a judge and the attorney for the defence become 'friends' on Facebook, and discussed the case in question using Facebook during the court case. As a result of an earlier ruling on the freedoms of the press within court rooms the London Riots saw widespread use of Twitter by the media to report on live court proceedings during the chaotic court days following the commencement of civil disorder (Goodman 2011).

A number of laws have a bearing on the London riots, prominent points on which are explored below:

Although rarely enforced, the Counter Terrorism Act of 2008 (UK Government 2008) contains provisions to prevent members of the public from taking photographs of police officers in public. However, the provisions

were designed to counter terrorism, and the prominence of the police in online footage relating to the riots ensured that police actions are highly visible to the world (Etling, Faris & Palfrey 2010)..

The Communications Act of 2003 (UK Government 2003) has been used in the past to prosecute those who have posted illegal information on social networking sites. One of the first widely publicised cases related to a man antagonised by the closure of his local airport, who posted on Twitter that he would “blow it up”, who was reported to the police by the airport management (Brooke 2010).

The Regulation of Investigatory Powers Act (RIPA) 2000 (UK Government 2000) is the primary Act the police use to request communications data from SNS in order to conduct investigations. Interestingly, RIPA does not require the originator of the data to be informed that it has been the subject of a RIPA request.

The UK government have the power to block websites which infringe copyright through the court system using the Digital Economy Act of 2010 (UK Government 2010). They also have the right remove content which contravenes the Terrorism Act of 2006 (UK Government 2006). However, it is unclear whether the government could legally block services such as Twitter, Facebook, etc.

4 Future trends and their implications

SNS have evolved considerably in the last decade, and will continue to do so in future. The ongoing evolution of services could affect users and the law enforcement community in a number of ways. Some of the prominent issues in this area include:

Increased use of artefact geotagging using mobile equipment (photographs, blog and micro blog posts etc) using inbuilt GPS receivers, or triangulation. The lack of user awareness for default settings for geotagging could cause privacy issues. Geotagging is turned on by default on platforms such as the iPhone camera, and are off by default on others such as Twitter. However, the resource implications for such data use in investigations are considerable.

Live SNS data mining tools are now common, including tools such as Monitter¹² for Twitter. Recent research in this area shows that civil disturbances of the type seen during the London Riots could potentially be predicted in advance (Lansdall-Welfare, Vasileios & Cristianini 2012) given sufficient resources. There is a clear issue with members of the public wanting to report crime via social networking despite being told not to do so. There are also issues relating to the lack of trained online SNS monitoring police staff (Metropolitan Police Service 2011)

Increased use of video uploads rather than textual information poses a considerable problem for future law enforcement. YouTube video uploads in 2010¹³ amounted to 13 million hours of footage, over double that uploaded in 2009. Forensic examination of video footage is considerably more complicated than text. It has been estimated that over 40,000 hours of video footage were gathered during the London Riots (Halliday 2011). The footage could take years to examine, collate and categorise. Academic research (Sarfraz, Zafar & Edirisinghe 2011) (Senior 2009) (Dee, Velastin 2008) in this area may well provide automated and semi-automated solutions to the problem, however they are unlikely to do so in the near future, causing a capability gap which could cause a considerable drain on human resources.

5 Future Work and Conclusions

Evidence has shown the use of online SNS to organise, defend against and monitor civil disturbances. Although focussed primarily on one of the largest civil disturbances to occur in the UK, the London riots of 2011, the paper has drawn on other examples from across the world highlighting a global issue.

It is arguable that the information currently being analysed in support of legal cases is already stretching the resources of the law enforcement system as it currently stands. In particular it is clear that the government will need to embrace the use of new services to support reporting by the public of issues encountered, monitoring by the police, and efficient, procedurally acceptable evidence gathering from social networking media.

¹² Monitter www.monitter.com Accessed 26/3/2013

¹³ YouTube www.youtube.com/t/press_statistics consulted 7/9/2011

It will also be necessary to determine new methods and techniques to support categorising, analysing and storing evidence for online social networking investigations. In addition the growth, evolution and potential disruptive use of online SNS will continue to evolve our understanding of information and systems theories, and significant potential exists for more long-term studies into the use of online SNS for disruptive purposes.

References

- Amparo, L. & Martínez de Albéniz, I. 2009, "'An Original Protest, at Least' Mediality and Participation" in *Cultures of participation. media practices, politics and literacy (Participation in Broadband Society)*, eds. G. Hajo, H. Larissa, L. Amparo & L. Claire, 1st edn, Peter Lang Pub Inc, New York, pp. 141-158.
- BBC News 2011a, 8/15/2011-last update, *Looting suspect traced on Facebook by stolen laptop's owner* [Homepage of BBC], [Online]. Available: <http://www.bbc.co.uk/news/uk-england-london-14536870> [2011, 8/15].
- BBC News 2011b, 8/11/2011-last update, *Riots: Benefits e-petition hits crucial 100,000 mark* [Homepage of BBC], [Online]. Available: <http://www.bbc.co.uk/news/uk-politics-14474429> [2011, 8/11/2011].
- BBC News 2011c, 8/19/2011-last update, *Social networks to meet home secretary over riots* [Homepage of BBC], [Online]. Available: <http://www.bbc.co.uk/news/technology-14587502> [2011, 8/19].
- BBC News 2011d, 8/10/2011-last update, *Three killed protecting property during Birmingham riots* [Homepage of BBC], [Online]. Available: <http://www.bbc.co.uk/news/uk-england-birmingham-14471405> [2011, 10/8].
- Bilge, L., Strufe, T., Balzarotte, D. & Kirda, E. 2009, "All your contacts are belong to us: automated identity theft attacks on social networks", *Proceedings of the 18th international conference on World wide web* New York, pp. 551.
- Boyd, D. & Ellison, N. 2007, "Social Network Sites: Definition, History, and Scholarship", *Journal of Computer-Mediated Communication*, vol. 13, no. 1, pp. 210-230.
- Brooke, C. 2010, 1/19/2010-last update, *Frustrated air passenger arrested under Terrorism Act after Twitter joke about bombing airport* [Homepage of Daily Mail], [Online]. Available: <http://www.dailymail.co.uk/news/article-1244091/Man-arrested-Twitter-joke-bombing-airport-Terrorism-Act.html> [10/07/2011, 10/07].
- Cameron, D. 2011, 8/11/2011-last update, *Public Disorder* [Homepage of Hansard, House of Commons], [Online]. Available: <http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110811/debtext/110811-0001.htm#1108117000001> [2011, 8/11].
- Cayley, S. 2009, *Flash Mobs and Urban Gaming: Networked Performances in Urban Space*, Dissertation, McGill University.
- Dee, H. & Velastin, S. 2008, "How close are we to solving the problem of automated visual surveillance?", *Machine Vision and Applications*, vol. 19, no. 5, pp. 329-343.
- Emerson, R. 1976, "Social Exchange Theory", *Annual Review of Sociology*, vol. 2, pp. 335-362.
- Erdbrink, T. 2012, *Iran increasingly controls its Internet*, 9th February edn, The Washington Post, Washington DC.
- Etling, B., Faris, R. & Palfrey, J. 2010, "Political Change in the Digital Age: The Fragility and Promise of Online Organizing", *SAIS Review*, vol. 100, no. 2, pp. 37-49.
- Facebook 2011, 9/4/2011-last update, *Statistics* [Homepage of Facebook], [Online]. Available: <http://www.facebook.com/press/info.php?statistics> [2011, 9/4/2011].
- Fassahi, F. 2009, 12/3/2009-last update, *Iranian Crackdown Goes Global* [Homepage of The Wall Street Journal], [Online]. Available: <http://online.wsj.com/article/SB125978649644673331.html> [2011, 8].
- Fogel, J. & Nehmad, E. 2009, "Internet social network communities: Risk taking, trust, and privacy concerns", *Computers in human behaviour*, vol. 25, no. 1, pp. 153-160.
- Goodman, D.J. 2011, *Following the Parade of Accused British Rioters on Twitter*, 12th August edn, The New York Times, New York.
- Gross, R., Acquisti, A. & Heinz III, J. 2005, "Information revelation and privacy in online social networks.", *Proceedings of the 2005 ACM workshop (WPES '05)*, eds. V. Atluri, De Capitani di Vimercati, Sabrina & R. Dingledine, ACM, , June 30th, 2005, pp. 71.
- Halliday, J. 2011, *UK riots: Met police pressure media to hand over videos and pictures*, 30th August edn, The Guardian, London.
- Handley, M. 2010, 2/18/2010-last update, *How Prisoners Harass Their Victims Using Facebook* [Homepage of Time Magazine], [Online]. Available: <http://www.time.com/time/business/article/0,8599,1964916,00.html> [2011, 10/4].
- Kelly, S. & Cook, S. 2011, *Freedom on the net 2011, A Global Assessment of Internet and Digital Media*, Freedom House.
- Krishnamurphy, B., Gill, P. & Arlitt, M. 2008, "A Few Chirps About Twitter", *WOSN '08 Proceedings of the first workshop on Online social networks*, pp. 19.
- Laer, J. & Aelst, P. 2009, "Cyber-protest and civil society: the Internet and social movements action repertoires in social movements" in *The Handbook on Internet Crime*, eds. Y. Jewkes & M. Yar, 1st Edition edn, Willan Publishing, Abingdon, pp. 230-254.
- Lansdall-Welfare, T., Vasileios, L. & Cristianini, N. 2012, "Effects of the Recession on Public Mood in the UK", *WWW 2012 – MSND'12 Workshop* Lyon, pp. 1221.
- Livingstone, S. 2008, "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression", *New Media and Society*, vol. 10, no. 3, pp. 393-411.
- May, T. 2011, 8/11/2011-last update, *Theresa May: speech on riots* [Homepage of The Home Office], [Online]. Available: <http://www.homeoffice.gov.uk/media-centre/speeches/riots-speech> [2011, 10/4].
- Mcillwain, J.S. 1999, "Organized crime: A social network approach", *Crime, Law & Social Change*, vol. 32, pp. 301-323.

- Metropolitan Police Service 2011, *Strategic Review into the Disorder of August 2011*, The Metropolitan Police Service, London.
- Milivojevic, S. 2011, *Social Networking Sites and Crime: Is Facebook more than just a Place to Procrastinate?*, Sydney Institute of Criminology, Sydney, Australia.
- Nelson, S., Simek, J. & Foltin, J. 2009, *The Legal Implications of Social Networking*, Sensei Enterprizes Inc.
- Nisbet, E. 2008, "Media Use, Democratic Citizenship, and Communication Gaps in a Developing Democracy", *Int.Journal of Public Opinion Research*, vol. 20, no. 4, pp. 454-482.
- Nosko, A., Wood, E. & Molema, S. 2010, "All about me: Disclosure in online social networking profiles: The case of FACEBOOK", *Computers in Human Behavior*, vol. 26, no. 3, pp. 406-418.
- Obar, J., Zube, P. & Lampe, C. 2012, "Advocacy 2.0: An Analysis of How Advocacy Groups in the United States Perceive and Use Social Media as Tools for Facilitating Civic Engagement and Collective Action", *Journal of Information Policy*, vol. 2, pp. 1-25.
- Pettifor, T., Gregory, A. & Layton, J. 2011, 8/10/2011-last update, *UK riots: Untraceable BlackBerry Messenger should be suspended, claims Tottenham MP David Lammy* [Homepage of The Mirror], [Online]. Available: <http://www.mirror.co.uk/news/top-stories/2011/08/10/uk-riots-tottenham-mp-david-lammy-calls-on-blackberry-to-suspend-network-to-stop-rioters-organising-trouble-115875-23333287/> [2011, 10/4].
- Robards, B. 2010, "Randoms in my bedroom: Negotiating privacy and unsolicited contact on social network sites", *PRism Online PR Journal*, vol. 7, no. 3.
- Rosenblum, D. 2007, "What Anyone Can Know. The Privacy Risks of Social Networking Sites", *IEEE SECURITY & PRIVACY*, vol. 5, no. 3, pp. 40-49.
- Sarfraz, M.S., Zafar, I. & Edirisinghe, E.A. 2011, "Real Time Automatic License Plate Recognition for CCTV Forensic Applications", *Journal of Real-Time Image Processing, Springer, 2011*, vol. To Appear.
- Senior, A. 2009, "An Introduction to Automatic Video Surveillance" in *Protecting Privacy in Video Surveillance*, ed. A. Senior, First Edition edn, Springer, London, pp. 1-9.
- Sewell, G. 1998, "The Discipline of Teams: The Control of Team-Based Industrial Work through Electronic and Peer Surveillance", *Administrative Science Quarterly. Special Issue: Critical Perspectives on Organizational Control*, vol. 43, no. 2, pp. 397-428.
- Shanahan, J. & Morgan, M. 1999, *Television and Its Viewers: Cultivation Theory and Research*, 1st edn, University of Cambridge, Cambridge.
- Somaiya, R. 2011, 8/13/2011-last update, *After British Riots, Conflicting Answers as to 'Why'* [Homepage of The New York Times], [Online]. Available: <http://www.nytimes.com/2011/08/14/world/europe/14looters.html> [2011, 10/4].
- The Crown Prosecution Service 2011, 8/16/2011-last update, *CPS statement on conviction of two men over incitement on Facebook* [Homepage of The Crown Prosecution Service], [Online]. Available: http://www.cps.gov.uk/news/press_statements/cps_statement_on_conviction_of_two_men_over_incitement_on_facebook/ [2011, 8/16].
- The Federal Communications Commission 2012, *FCC*, FCC.
- The Mirror 2011, 8/22/2011-last update, *UK riots: man aged 70 arrested for looting a Sainsbury's* [Homepage of The Mirror], [Online]. Available: <http://www.mirror.co.uk/news/top-stories/2011/08/22/uk-riots-man-aged-70-arrested-for-looting-a-sainsbury-s-115875-23362734/> [2011, 8/22].
- Tokunaga, R. 2011, "Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships", *Computers in Human Behavior*, vol. 27, no. 2, pp. 705-713.
- UK Government 2010, *Digital Economy Act of 2010*, Law edn, UK, UK Parliament.
- UK Government 2008, *Counter-Terrorism Act 2008*, Law edn, UK, UK Parliament.
- UK Government 2006, *Terrorism Act of 2006*, Law edn, UK, UK Parliament.
- UK Government 2003, *The Communications Act of 2003*, Law edn, UK, UK Parliament.
- UK Government 2000, *The Regulation of Investigatory Powers Act (RIPA) 2000*, Law edn, UK, UK Parliament.
- UK Government 1994, *Criminal Justice and Public Order Act 1994*, Law edn, UK, UK Parliament.
- UK Government 1990, *Computer Misuse Act 1990*, Law edn, UK, UK Parliament.
- Wikipedia 2011, 8/23/2011-last update, *Flashmob* [Homepage of Wikipedia], [Online]. Available: http://en.wikipedia.org/wiki/Flash_mob [2011, 8/23].