Enhancing public security through use of social media: the good, the bad and the ugly

Abstract
This paper focuses upon the emerging findings of a recently completed Horizon 2020 project -MEDI@4SEC: The Emerging Role of New Social Media in Enhancing Public Security. Working actively with police forces across Europe, MEDI@4SEC has created a future roadmap for the role of social media in law enforcement and public security planning, not only for communication purposes and as a listening platform, but also as a tool for collaboration – a digital realm where policing and crime prevention can be done in new ways with new types of digital and real-world interventions. The ongoing results of MEDI@4SEC presented here illuminate a variety of police tasks that are increasingly utilising social media. Such activities further highlight a series of challenges and opportunities for policing associated with organisational change, legal and ethical issues, privacy, transparency and liability, technological infrastructure and training required and budgetary concerns that are likely to shape the take up of social media usage in police forces around Europe in the coming years.
Keywords: social media, ethics, community policing

Introduction

Nothing will ever replace good old fashioned police work, but Facebook and Twitter have been like a tool on our belt, in some ways it can help them in their investigations and in some ways it can hinder - Bill Bratton (Former NYPD Commissioner)

This paper focuses upon the emerging findings of a recently completed Horizon 2020 project - MEDI@4SEC: The Emerging Role of New Social Media in Enhancing Public Security. Working actively with police forces across Europe, MEDI@4SEC has advanced a future roadmap for the role of social media in law enforcement and public security planning, not only for communication purposes and as a listening platform, but also as a tool for collaboration – a digital realm where policing and crime prevention can be done in new ways with new types of (digital and real world) interventions (Foster, 2016).

The MEDI@4SEC project has addressed three key questions which are illuminated in this paper: How and why new forms of social media currently are being adopted and used by policing, public security planners and citizens; how social media use amongst law enforcement authorities should evolve in the future and influence operational practices and requirements; and what the social, ethical, legal and data protection implications are of this increased use of social media by the police.

Social media is omnipresent and have become powerful mechanisms driving social, and economic change. New and emerging forms of social media (e.g. Twitter, Facebook, YouTube, Instagram and others) are open, distributed, digital communication platforms that enable individuals and communities of users to create and share information and ideas worldwide. Social media allows the fast sharing of user generated content, facilitating communication on a many-to-many basis, providing the ability for personalization and anonymity and allowing use anytime and anywhere (De Vries and Smilda, 2014; Bartlett et al 2013). Specifically, in relation to policing, social media allows law enforcement authorities and others involved with public security to ask for information from, send information instantaneously to and interact with a range of civil society groups as well as providing a monitoring and intelligence gathering function (Schneider, 2016).

This paper draws from studies conducted during the Medi@4sec project which was funded from the European Union’s Horizon 2020 Programme for research under grant agreement no 700281. The collaborative work of all consortium partners in this paper is acknowledged, details of which can be found at www.mediac4sec.eu. The work of the project, including a range of detailed research reports on themes explored in this paper can also be found on this website. Follow @media4sec on twitter for further updates.
The growing role of social media in policing tasks

The MEDI@4SEC project focuses upon understanding the opportunities, challenges and ethical considerations of enhancing social media use for public security: the good, the bad and the ugly. The good comprises using social media for problem solving, fighting crime, decreasing fear of crime and increasing the quality of life. The bad is the increase of digitised criminality and terrorism with new phenomena emerging through the use of social media, particularly on the dark web. The ugly comprises the grey areas where trolling, cyberbullying, threats, or live video-sharing of tactical security operations and the propagation of rumours are phenomena to deal with during incidents. Making use of the possibilities that social media offer - including smart ‘work-arounds’ - while respecting privacy, legislation and ethics is not an easy task.

This changing situation raises a series of challenges and possibilities for overall policing and has impacted upon a range of specific policing tasks, notably around communication, engagement and community policing, response to emergencies and crisis, surveillance and, criminal investigations and intelligence gathering. In terms of communication and engagement social media has changed the landscape of policing communication drastically (Goldsmith, 2015) enabling everyone to send information or ask questions to anyone, instantaneously and at minimal costs. This is true for both internal police communications as well as increasing accessibility of policing services for citizens. The two-way engagement with the public is a tangible benefit of social media. In stimulating engagement between police and community, social media adds legitimacy and knowledge to many police tasks and can offer a great opportunity to reach target groups who traditionally are hard to reach. In response to a reduction in ‘on the beat’ policing, individual police officers are increasingly using social media to enhance their visibility and reassure the public that they are active in an area, as well as making it easier for the public to contact them. In this way, increased social media communication can lead to increased transparency and increases in perceived police legitimacy and reputation (Meijer and Thaens, 2013; Grimmelikhuijsen, & Meijer, 2015).

Conversely, social media can also damage reputation, for example in cases where the misbehaviour of police officers is recorded and shared through social media. Though fruitful for different purposes, communication using social media thus generates challenges and training needs for police forces. One challenge with communication via social media is finding the right tone for the conversation. Information needs to be relevant and useful for citizens, otherwise the public might be left with the impression that the police are not spending their time effectively. There are different ways for police forces to communicate via social media; some try to be more personal and others more formal. Many studies highlight that the public would like to see more engagement (two-way interaction), while current practice in many countries sees the police use social media mostly to
send or gather information for fear of misusing it and getting censured, and not for fully interacting with the public (Heverin & Zach, 2010).

Social media can furthermore stimulate community policing, by enabling all employees in a police organization to have fast and (almost) autonomous contact with citizens (Lieberman et al., 2013; Meijer & Thaens, 2013). In theory, better communication enables ‘active citizenship’ which itself enhances effective community policing in ways that allow citizens give the police information through social media and in some cases help with investigations (De Vries & Smilda, 2014). Neighbourhood police officers for example, often use Twitter and Facebook extensively to obtain information from their community. Social media can also be used to motivate the crowd to volunteer. For example, the restoration of public places that have been affected by riots or demonstrations, as seen in the ‘clean up’ after the London 2011 riots (Procter et al 2013). Another way for the community to stimulate community policing is by organizing ‘neighbourhood watch’ through a WhatsApp group or a commercial service like Nextdoor (De Vries, 2016). Such community policing practices are not unproblematic. Challenges may arise around privacy and vigilantism, posing critical ethical questions about the roles and responsibilities of citizens who get involved in crime prevention (Huey at al. 2012)2.

A further core police task that increasingly utilises social media is responding to emergencies, incidents and crises. In the case of an emergency, incident or crisis, community members need to be able to contact and inform the police quickly, and the police need to achieve situational awareness in a short space of time. An array of mobile apps have also been launched to warn bystanders of incidents and enable them to act as first responders. However, using social media to alert police to an emergency situation is complex and challenging. It requires the public to respond quickly and for police forces to have appropriate technical systems that can interpret and act upon the data received. In the case of larger incidents, police officers can use social media to warn and inform large number of citizens simultaneously by sending a small number of messages that then get spread. For example, during the Christchurch earthquake in New Zealand and the flooding in Queensland, Australia, (both 2011) social media was the primary medium to broadcast information. After the recent spate of urban terrorist attacks across Europe social media was used to share information with the community and to keep them informed about the ongoing incident (Coaffee, 2017). During a crisis, social media is not only a helpful communication tool but also enables police to gather and analyse a lot of information in a short time period. However, social media also causes problems for police responding

2 Helped by scientific research of funded through the EU Horizon 2020 programme police forces are now discussing the next generation of community policing, allowing them to engage with virtual instead of just local communities and shifting from citizen participation (where citizens volunteer to join police activities) to police participation (where police joins activities initiated by the public). See for examples the INSPEC2T, Trillion, Unity and CityCop projects.
to incidents in terms of having to expend a lot of time and resources quelling rumours whilst an event is ongoing, which can cause considerable disruption to policing activities and in some cases compromise attempts by police to track suspects as they move away from the scene of an incident (ibid).

Surveillance tasks can be significantly affected by social media and aid the police in preventing unrest and signalling suspicious situations. By monitoring social media alongside other sources such as CCTV, police can better get to know certain communities and their behaviours and pick up leads of potential incidents or planned criminal activity. Emerging research has highlighted that analysing large numbers of tweets can improve crime prediction, help make deployment decisions and increase effective allocation of resources (Gerber, 2014). However, police must know how to effectively monitor these types of communications in order to gauge the mood of a crowd, assess whether threats of criminal activity are developing and to stay apprised of any plans by large groups of people to move to other locations. The emerging challenge in policing of using social media for online ‘surveillance’, particularly of monitoring terrorist groups who use social media to radicalise and recruit, illuminates the scale of the challenge facing police forces both in terms of technical equipment requirements and also in training to better be able to analyse social media. For example, in the aftermath of a serious incident, police can “mine” social networking sites to identify victims, witnesses, and perpetrators that which requires getting hold of the provenance of messages, understanding where the information is coming from and if it can be trusted.

The police task of tracking down the offenders of crimes - criminal investigation - increasingly utilises social media to achieve its goals. By leaving traces on social media criminals turn it into a potentially rich source of incriminating information that can be collected and analysed in accordance with legal protocol. Overall, social media has proved to be helpful in solving crimes. This has often involved regularly visiting and monitoring of certain sites that are infamous for being used to facilitate criminal activity (e.g. the dark web) and those which allow or stimulate hate propaganda. However, increasingly, police officers are seeking to translate existing legal frameworks, developed for police operations in the physical world into digital legal frameworks because the crucial legal framework for investigations on social media is missing (Denef, et al., 2012). Therefore, the challenge for online investigation is to obtain accurate data legally from the different social media networks, which have different methods of sharing data (or not sharing) with the police.

The police further use social media for intelligence operations. The speed of social media provides a crucial advantage when appealing for witnesses, or, information or looking for missing persons. For example, social media can be used to assist with missing persons’ inquiries by enabling the police to harness the ‘wisdom of the crowd’ (Denef et. al., 2012). But although social media can be helpful in intelligence gathering, it also brings forward
challenges concerning the veracity of the intelligence obtained (Kumar 2013). Identifying credible information from rumours and speculation is proving increasingly difficult. Filtering and identifying the useful information in a situation of information overload often creates provenance and trust issues.

**Challenges and opportunities of social media use in practice**

During the course of the MEDI@4SEC project we have investigated the enactment of these different policing tasks though a series of thematic workshop where a range of policing and non-policing stakeholders have discussed and debated the key challenges and opportunities of using social media in these different practice contexts.

Firstly, our workshop on Do-it-yourself (DIY) policing questioned the general division of responsibilities and legitimate power between citizens and police. For some policing activities a key question is about how to cooperate with citizens, when to take control and how to avoid negative effects. For example, there is a growing trend of citizens taking coordinated action in places where there is a perception that public security falls short or fails, for example with the growth of so-called ‘paedophile hunting’ (Jamieson, 2016). This leads to the question of whether DIY policing can actually assist police operations. Whilst some European police forces have taken concerted efforts to co-create safety jointly with citizens, DIY policing does raise a range of delicate ethical questions. Empowered citizens have the means to fight injustice and produce desirable change, while at the same time they can also create great harm when acting irresponsibly or taking the law into their own hands.

Secondly, we looked at the opportunities and challenges for social media use within the context of riots and other mass gatherings and in particular the role social media played in monitoring, signalling and communicating with the public during such events (see for example Archie, 2016; Mair, 2016 for terrorist attacks). In such situations, the rapid adoption of social media has assisted in the organization and coordination of the event itself, as well as its policing. This raises key questions about authoritatively communicating with the public in such situations and the advancement of a communication strategy to ensure the uniform use of social media by authorities in a positive, friendly, instructive and helpful tone to promote citizen engagement, collaboration and trust. Such interactive communication can provide a substantial resource that can aid situation awareness but should be done in an ethically aware way that protects data privacy and avoids spreading unsubstantiated rumours.
Thirdly, we focused upon the everyday policing of public security, including cooperation with citizens via social media as part of new models of ‘community policing’. The transformed communication and information habits brought forth by social media, provides policing with new opportunities for intelligence sources and platforms to communicate as well as enhance their local crime prevention strategies (Ruddell and Jones, 2013; LexisNexis, 2014). But how can community policing initiatives supported by social media best contribute to the everyday management of security? And how can policing advance a unified, consistent approach to modern technology usage, incorporating specialized staff, budget dedicated to innovation and defining a clear legal framework and procedural protocols?

The fourth and fifth themes explored focused upon newly emerging areas of policing: dark web investigations and trolling. Historically, technology has revolutionized policing practices but more recently it has also facilitated criminality with the Dark Web emerging as a key space for ‘high tech’ (organized) cybercrimes linked, for example, to cryptomarket-related crime or the distribution of extremist material, that raises a number of issues for police forces to consider: keeping one step ahead of the cyber-criminal; assessing the balance between freedom of speech and crime facilitation with regard to dark web content; as well as issues of jurisdiction that is forcing co-ordinated international efforts to be put in place (Bryant, 2014; Trottier, 2015). With regard to trolling – broadly understood to include cyberbullying, cyberhate, cyberstalking, cyberharassment, revenge porn, sex-tortion, naming and shaming and flaming – European police forces are coming to terms with its legal status - something which differs from jurisdiction to jurisdiction and from act to act. The relationship between the formal policing of trolling by police and community-driven counter-trolling actions is also coming under scrutiny with questions being asked about where the responsibility – both legal and moral – for intervention lies. It also poses questions about how police can improve their human and technological resources to intervene in trolling effectively, and what legal and policy frameworks should be developed to assist and facilitate the countering of trolling. For both dark web and trolling activities there is also a broader question about the role which social media providers should play in policing illegal activity, extremist material and online abuse, in large part because it happens on their platforms and because they have the discretion to remove material. These questions have recently been tested in Germany through the introduction of the controversial Netzwerkdurchsetzungsgesetz (NetzDG) law which came into force in January 2018 and requires more effective policing of social media after several high-profile cases in which inappropriate material was being spread via the German arms of prominent social media firms. 3 However, adjudicating on what falls foul of hate-speech laws and what is legitimate freedom of expression is proving difficult to decipher.

---

3 The new law gives the networks 24 hours to act after they have been told about law-breaking material (BBC, 2018).
The sixth theme we focus on cross cuts the others and highlights innovative market solutions and new commercial products for including social media in police work. To digest, analyse, expand and share the valuable information on social media for policing, constant innovations are required in order to meet expanding and complex needs. Such applications should not only aim to increase the effectiveness of policing operations with fast and accessible formats but do so in ways that respect data protection regulations. Ethical and societal considerations and privacy by design technologies thus need to be at the forefront of new solutions to ensure police use of social media cannot be above the law.

Emerging trade-offs in police use of social media

The 2017 UK Home Affairs Committee inquiry into Policing for the future: changing demands and new challenges noted that advances in technology and notably social media have ‘led to the emergence of new forms of crime, and have enabled other crimes to move online, changing their nature and impact on victims and communities. Technological change has also generated new opportunities for the police at a time of increasing focus on efficiency and innovation’ (HAC, 2017). Given the predicted future state of policing across Europe, many police organizations adopting social media consider the usage very fruitful for different purposes in their operational tasks and organizational goals (de Smet 2012). Whilst the use of social media has brought forward tremendous benefits, there are significant challenges and trade-offs. Most immediately, and from a resourcing perspective, being present on and using data from social media takes a lot of time effort and in many cases specialist equipment/tools, a conflict with Europe-wide cutting of police-budgets (The Police Foundation, 2014).

A further emerging challenge concerns significant issues of ethics and law particularly with regard to data sharing and privacy that have not traditionally been a major concern for police forces. This is leading to ongoing discussion about the need for guidelines or codes of conduct to adhere to or consider before individual police offices tweet or share Facebook messages (Mulder, 2018). Whilst the social media platforms utilised by policing can facilitate communication, interaction and participation on an unprecedented scale and deliver security more effectively and efficiently, all that glitters is not gold. Social media is also the catalyst and conduit for abusive communication, for the grooming of children for sexual exploitation, for terrorist recruitment and for a range of other unethical and illegal activities. Moreover, anonymity and encryption can help some criminals act with impunity. And, although everyone agrees that police should take measures to detect, prevent and prosecute such behaviour, such measures are often controversial, risking disproportionate interference with freedom of expression or privacy, or the unwarranted visitation of suspicion on innocent individuals or groups. Inaccurate or incom-
plete information and the problematic inferences about people’s criminality that follow can further result in disproportionate monitoring or even unfair criminalization.

It is therefore important that police adopting social media as a core activity address how such tools can address risks of bias, such as in the patterns of language that it flags as suspicious and what safeguards can be built in to prevent their misuse. In a recent example from the USA, responses to freedom of information requests from the American Civil Liberties Union have revealed that data mining companies that marketed products specifically to target activists of colour or religion have had contracts with a number of police forces. In these instances data from Twitter, Instagram and Facebook was used to surveil, monitor and track protest groups, including the Black Lives Matter campaign and Muslim protestors using specific hashtags such as #MuslimLivesMatter (Cagle, 2016; Perez, 2018).

Balancing the detection and prosecution of crime with ethical concerns is emerging as a core tension within social media use in policing. Through the MEDI@4SEC project we have identified a range of issues with police use of social media that could possibly subvert European ethical and legal norms of democracy. These issues include accountability, transparency, fairness and duties of special care for the vulnerable in the application of criminal justice. They further include a proper respect for civil liberties, and the ethically risky, anti-social and illegal uses of social media by citizens. These issues implicate not only the duties and functions of public security providers such as police and local authorities but also the potential role of technology developers and social media providers as evidenced by calls from senior politicians throughout Europe to pressurise prominent social media companies to remove extremist material. As the British Prime Minister noted in June 2017 after a year of terror attacks across Europe, ‘we cannot allow this ideology the safe space it needs to breed, yet that is precisely what the Internet and the big companies that provide Internet services provide’ (cited in Stone, 2017). Subsequently the UK government have worked with technology companies to develop a new tool that can automatically detect terrorist content on any online platforms with a high degree of accuracy (UK Home Office, 2018).

Further ethical issues include, in particular, risks of disproportionate interference with the privacy of innocent individuals, risks of outright discrimination or unwarranted stigmatisation of individuals or groups as criminally suspicious as well as risks of discrimination and unfair (because less easy or reliable) access of some vulnerable or disadvantaged groups to criminal justice or public security resulting from their relative lack of technology and/or technological skills. In addition, the rights of police officers to a private life and to freedom of expression on social media are also emerging as key issues to consider as allegations emerge in the media of inappropriate use of social media by officers through abusive postings or the leaking of confidential information (Irish Times, 2018).
Furthermore, the involvement of citizens in the provision of public security and criminal justice raises significant concerns from a legal perspective. These relate primarily to the difficulty of ensuring transparency, accountability and non-discrimination in the delivery of public security when functions are carried out by citizens driven by their own interpretations of the law and morality and without democratically legitimised authority. For example, in the UK a complex debate has raged over the extent to which the police should work with self-styled paedophile hunters - who for some are vigilantes or ‘digilantes’ acting outside of the law but for others could be a source of useful information that is increasingly used in prosecutions. These concerns are likely to persist and indeed grow as it becomes apparent that the police are unable - for a range of reasons - to deal with the proliferation of illegal and unethical behaviour online. Key challenges and risks for public security providers in responding to such behaviour, including on the Dark Web, include distinguishing between illegal and merely offensive or otherwise unethical behaviour, and determining the line between justified covert interactions with criminals and unjustified entrapment.

Mainstreaming social media in policing

Social media has added another dimension to the police tool-belt and has been a powerful force in driving organisational change within police departments (Lierbeman et al 2013; Meijer & Thaens 2013). However, the introduction of social media in policing has shown differences in the conditions required for success in adopting social media as a mainstream activity and the respective opportunities and threats this has presented. A European wide survey conducted with senior policing respondents elicited a series of needs, priorities and concerns about using social media now, and in the future. Specifically, it illuminated a series of important and inter-linked considerations that will either facilitate or stymie social media use by police forces in the near future. These are shown in Figure 1 below.
Enhancing public security through use of social media: the good, the bad and the ugly

**Figure 1:** Key factors for the uptake of social media in policing

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater engagement with the public</td>
<td>Engagement between LEAs and the public through social media will increase two-way communication and enable valuable security information to be exchanged.</td>
<td>LEAs will have greater situational awareness ‘on the street’ and citizens will contribute to, and be better informed about, security issues.</td>
</tr>
<tr>
<td>Changes in public opinion</td>
<td>The changes in the way public perceives the trade-off between privacy and safety will impact the way social media is used for public security planning.</td>
<td>In the future, the public may have a different perspective on how important privacy actually is with respect to the trade-off between privacy and safety.</td>
</tr>
<tr>
<td>Perception of usefulness and ease of use</td>
<td>Social media will become increasingly easy to use in a range of situations.</td>
<td>Individuals / community will be encouraged to use social media as long as they feel confident that they contribute to, and in return receive, “public security”.</td>
</tr>
<tr>
<td>Social media popularity in LEAs</td>
<td>The perceived importance of social media for public security will influence the viability of the presence of LEAs in social media platforms as well as the prevalence of private social media accounts.</td>
<td>Active interaction and enrolment in LEAs social media accounts will be an important metric of the successful implementation of the venture.</td>
</tr>
<tr>
<td>Law enforcement agency re-organization</td>
<td>Re-engineering of procedures, processes, human and technology resources is needed in order to embed social media within their existing organizational structures.</td>
<td>Develop social media strategies and plans to respond and react effectively in everyday policing operations and emergency situations.</td>
</tr>
<tr>
<td>Privacy, transparency and liability concerns</td>
<td>Privacy, transparency &amp; legal liability regarding the use, misuse and errors in the management of information and practices followed by LEAs in social media.</td>
<td>Transparency between public authorities and LEAs will play an important role in the way citizens embrace social media. Legal liability &amp; clear definitions of what information is collected and by whom is a significant component to transparency.</td>
</tr>
<tr>
<td>Changes in legislation</td>
<td>Future changes in legislation will impact the way social media is used for public security planning.</td>
<td>In the future, LEAs may have different restrictions on what information may be used and how for public security planning.</td>
</tr>
<tr>
<td>New technological advancements</td>
<td>New technologies will have a great influence on the activities and behaviour of citizens and organizations. Citizens rapidly adapt to new social media and leave previous ones behind.</td>
<td>Citizens will have more opportunities for networking and LEAs will have to be flexible in adapting social media in order to continue effective collaboration.</td>
</tr>
<tr>
<td>Financial burdens</td>
<td>Financial impact of the adoption, training, information upkeep and monitoring of social media platforms.</td>
<td>Budgetary restrictions can affect the number of staff and investment in technologies used for social media engagement by LEAs and its effective operation.</td>
</tr>
<tr>
<td>Infrastructure concerns</td>
<td>Social media technology tools and the related IT infrastructures needed, are under continuous development and evolution.</td>
<td>The appropriate IT infrastructure and tools to handle the continuously increasing needs of storage and processing of social media data produced.</td>
</tr>
</tbody>
</table>
From this analysis a number factors can be identified as key needs, notably advancing more user-friendly and user-attractive social media applications that are easier to use in policing. Also important in these new technological advancements are the ease with which community engagement and public relations can be facilitated through social media in a bi-directional way. Other key priorities that emerged centred upon how social media is bringing about significant changes in operations and practices and that assist police forces to become fully embedded into the digital world. Whist there is optimism about the impact and likelihood of change involving social media, a number of concerns remain prominent regarding how such change would be operationalized; notably around issues of data privacy, ethical and legal considerations, financial budgeting and the need for up to date infrastructure. In other words, whilst there is a ‘promise’ that social media will allow the police to do ‘more for less’ through efficiency gains and the facilitation of more joined-up and ethically-informed policing practices, the start up and running costs of such operations might affect the uptake of such techniques in future years.

References


• Ruddell, R., and Jones, N. (2013) Social media and policing: matching the message to the audience. Safer Communities, 12, 64-70.


