Happenings Foreseen: Social Media and the Predictive Policing of Riots*

Clemens Binder

Abstract: This article investigates the influence of Social Media platforms on policing protests and riots. Mainly, it is argued that through a stronger inclusion of Social Media data into policing, Social Media itself becomes a domain of internal security, therefore, it is argued, Social Media could become securitized itself. Another argument is that, as Social Media represents one aspect of the rise of Big Data in policing, law enforcement has shifted strategies from reaction to prevention, as the analysis of data offers the opportunity for predictive policing. In this article, law enforcement practices regarding Social Media in policing protests and riots are therefore investigated in order to assess if Social Media has caused a shift towards predictive policing and if this could be understood as a further securitization within internal security policy.

Schlagworte: Soziale Medien, Big Data, Open Source Intelligence, Predictive Policing, Innere Sicherheit
Keywords: Predictive Policing, Social Media, Big Data, Open Source Intelligence, Riot Policing

1. Introduction

„Predictive Policing“ – defined by Perry et al. (2013: 1pp.) as "*the application of analytical techniques—particularly quantitative techniques—to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions*" is emerging as tactics within police forces, especially in the US and the UK (Bachner/ Lynch 2016). Law enforcement agencies increasingly establish capabilities to cope with data from a variety of sources in order to detect, combat and prevent criminal actions. Big Data, one of the central evolving phenomena in today's world, is beginning to shape internal security policies of states and strategies of law enforcement. Predictive Policing is exemplary for this development and a fiercely debated topic.

Big Data, according to a report by the government of the UK, "*refers to both large volumes of data with high level of complexity and the analytical methods applied to them which require more advanced techniques and technologies in order to derive meaningful information and insights in real time*" (HM Government 2014: 2). As mentioned, Big Data represents a paradigm shift in the perspective on data, especially regarding its importance for various applications. Brooks (2013) describes "*data-ism*" as "*the rising philosophy of the day*"; for Boyd/ Crawford (2012: 663) it is obvious that "*[t]he era of Big Data is underway."* Cukier and Mayer-Schoenberger (2013a: 29) detect the evolution of the so-called "*datafication*", a development which quantifies social interactions and movements in order to facilitate the analysis of gathered data.

In this regard, the gathering of data from Social Media platforms is of particular importance. With a rapidly increasing number of users, Social Media has developed into a central means of communication and organization and is also perceived as means for policing and for protecting public safety and security. Therefore, the question arises if Social Media, as a facet of Big Data, has come to be used as an instrument of internal security policy. This would represent the politicization as well as securitization of a civil technology as well as a technologization of security as law enforcement agencies show increased dependence on technology in order to improve their methods. A concept which describes the increased significance of Social Media in security applications is the concept of Social Media Intelligence (SOCMINT) as defined by Omand et al. (2012).

This article will therefore assess if Big Data in general and Social Media in particular have developed into viable tools for internal security policy and, therefore, contain visible elements of securitization. The analysis will focus on the application of the SOCMINT concept on policing riots. In this context, predictive policing adds an interesting layer for analysis. Mainly, this article tries to answer two questions, first, if Social Media being used as means of law enforcement presents a process of securitization and second, how the inclusion of Big Data and Social Media has shaped policing protests, especially in the context of predictive policing.

2. Securitization theory and policing

As Big Data and Social Media are unpolitical in their respective nature, their usage in policing would represent a politicization of technologies, or even add an additional dimension, the dimension of securitization. As "*[s]ecuritization can […] be seen as a more extreme version of politicization*" (Buzan et al. 1998: 23) it is important to describe politicization briefly before defining securitization more thoroughly. Bijker (2001: 21) describes politicizing technology as a consequence of deeper understanding of technological culture and explicitly outlines the political dimensions of science and technology, in research as well as in its application. Bijker (ibid: 27) sees technology as a subject to social processes, interests, interactions and perceptions, technology then becoming politicized.

Securitization, as defined by Buzan et al. (1998: 23) means that an issue is considered an existential threat that requires emergency measures, whereas politicization means that an issue is part of the public policy agenda. Securitization occurs under different circumstances than politicization, as an issue area must be considered a threat to the integrity of the state.

---

*   This article has been double blind peer reviewed.

As the maintenance of public safety is considered central for the functioning of a state, securitization in the context of public safety is a possibility. Securitization, briefly explained, describes the social construction of security. The perception of threats is not an exogenous variable, as for example in realist theories, but constructed through discourses and actions. Wæver (1995: 55) regards security as a *"speech act"*, a process. Merely the expression of security concerns securitizes an issue, which, according to Wæver, leads to states being able to gain control on issues by defining them as a threat to security. However, as Williams (2003: 524) states not only language but predominantly images are essential for the social construction of security, as images shape security relations and perceptions. In this regard, the question arises to what extent Social Media has contributed to securitization, as images, news and debates spread quickly and create new perceptions of security, and especially if the securitization *through* Social Media leads to the securitization *of* Social Media.

Another approach that seems important in the regard of the social construction of security, especially when analyzing technological developments is the technologization of security. Ceyhan (2008: 120) views the *"promotion of technology as a security enabler […]"*, stating that technologies especially become means of securitized issues, for example border control. However, the increased usage of technologies as a means of security policy defines technologies as a critical infrastructure, for example in the cases of Information and Communication Technologies (ICTs). In consequence, this facilitates a securitization of technology, as technologies are exposed to substantial threats due to their importance for national security. Especially the case of Big Data signifies the importance of this problem, as data often contains sensible information about citizens and cannot only compromise privacy, but also personal security.

Assuming that the securitization of Social Media and Big Data is an emerging phenomenon, the question is how states and in this special case law enforcement units cope with these technological developments in order to maintain public safety, especially in the course of policing riots. In this regard it is important to understand general approaches towards policing and protest policing in particular. As predictive policing represents an intersection between Big Data and policing, the inclusion of data analytics and intelligence in police becomes central for the approach in this paper.

In the past, protest policing was more focused on the control of protest movements rather than on surveillance and early detection of such. McPhail et al. (1998) introduce two styles of protest policing – escalated force and negotiated management. Escalated force here describes a manner of policing where authorities use physical violence against protesters even if they act peacefully, whereas negotiated management establishes communication between protesters and authorities before protest movements in order to mitigate the danger of violent eruptions. Predictive policing adds the dimension of predicting riots by identifying risks out of different available data, for example historical evidence, potential rioters and events that could increase the likelihood of riots (see Perry et al. 2013: 10p.).

Earl et al. (2003) explain why authorities decide to police protests and how they act. They describe two crucial factors: threat and weakness that determine police action in protest movements. The perception of a movement as a threat might cause authorities to take more determined actions. Also, movements that are likely to collapse under pressure are sooner attacked. Earl et al. (2003: 584) furthermore describe an interdependence between threat and weakness, suggesting that police forces tend to take forceful actions against threatening, marginalized protest movements. In this regard, Big Data and Social Media can offer clearer insights into the structures of such movements and improve preparation. However, as Earl et al. (2003: 585) describe, police action is also dependent on the strength of the police force. *"Thus, large police departments with access to more resources will have a greater capacity to repress than will smaller forces with lower budgets and fewer officers."* This outlines a recurring obstacle in the effective use of Big Data: analytics are cost-intensive and require a great amount of resources, and especially smaller police forces could suffer from a lack thereof.

As Gill (1998) and Ratcliffe (2002) describe, intelligence has assumed a growingly important role in policing. Ratcliffe assesses that due to increasing crime rates, "intelligence-led policing" is one major development of policing, Gill describes a variety of reasons, such as organized crime and transnational developments that lead to a closer connection of social groups and societies. Intelligence-led policing can be understood as a process where data is not only collected, but analysed and disseminated according to common intelligence measures, it mainly means the application of the intelligence cycle[1] to law enforcement. Intelligence in policing therefore can be understood as *"the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality"* (Carter 2009: 11). Joh (2014: 35) states that *"the age of 'big data' has come to policing"*, meaning that policing focuses progressively on detecting future crimes by establishing data analytics, which proves the emergence of predictive policing.

At a first glance, securitization and policing might seem two very distinct topics. However, as policing is the primary means of combatting crime, and as crime is formulated as a threat through multiple discursive acts, it is a securitized issue. Policing can therefore be interpreted as a consequence of securitization, as well as technologization. Technologization as "security enabler" provides an opportunity to render policing more effective and ameliorate policing processes, for example intelligence-led policing profits greatly from increased use of technologies. The theoretical background allows a lens regarding the topic of Social Media in protest policing under a distinct point of view – using Social Media in the context of predictive policing would also signify a securitization of this technology, as the platforms do not only become an instrument for achieving security, but also an arena within which security-relevant interactions occur.

---

1 The intelligence cycle comprises four major steps – planning, collection, analysis and dissemination – and is the common way to describe intelligence processes.

3. Big Data and SOCMINT

The emergence of Big Data causes major shifts in a great variety of aspects of social and political spheres. For security, Big Data offers opportunities regarding intelligence collection, creating profiles of suspects and detect suspicious movements. As already stated, predictive policing signifies one aspect of law enforcement that has been affected by Big Data. A definition of Big Data can be found in the introduction of this article, however it is important to outline a number of aspects that describe problems and challenges regarding the phenomenon. Cukier and Mayer-Schoenberger (2013b: 94) outline the *"datafication of everything"*, the process of turning every domain of life, such as movements, texts and interactions, into data. Social Media facilitates datafication, as people share images and statements, create events and interact on these platforms, therefore, Social Media comprises a wide array of different data that is accessible fairly easily. This datafication runs parallel to a digitization of data, as increasing amounts of data are available in digital form (Joh 2014: 39). As the amount of data that can be collected from various sources is massive, Big Data has to fulfil a number of criteria in order to work as a functional instrument of security. Couch and Robins (2013: 5) define these characteristics as volume, variety, velocity, and veracity. Volume means that on a particular issue, a certain amount of data is required; variety defines that available data needs to cover a wider array of aspects of the issue; velocity depicts the requirement of quick availability; whereas veracity is explained as the validation and reliability of available data. These characteristics add a qualitative dimension to the quantitative nature of Big Data – it is not only advantageous being able to access great amounts of data, but this data in addition needs to provide useful information that is reliable. Reliability can be seen as the most important aspect of data quality, this could for example be achieved through the inclusion of multiple sources.

The significance of Social Media in the Big Data narrative is described by Lim (2016: 629) in that Social Media platforms *"have melded into a 'vast digital social commons' capable of facilitating complex analyses of sentiments, semantics, clusters and networks"*, that help to map criminal movements. As intelligence-led policing approaches have developed into a centrepiece of policing, law enforcement also makes use of Open Source Intelligence (OSINT), which describes processed Open Source Data and Open Source Information for intelligence purposes, meaning that a large amount of data available from easily accessible sources is evaluated with the purpose of improving knowledge on a variety of developments, for example in controlling protest movements. Social Media represents a facet of OSINT, as data is openly available. Intelligence gathered from Social Media however has become increasingly important that Social Media Intelligence has evolved as a distinct concept.

Social Media Intelligence (SOCMINT) can be defined as intelligence gathered from Social Media, following the definition of Scott/Jackson (2008: 22) of intelligence: *"[I]ntelligence is understood as the process of gathering, analysing and making use of information."* SOCMINT can therefore be interpreted as gathering data from Social Media Platforms, and then analysing it in order to address specific topics. Omand et al. (2012) describe five advantages for public security that emerge through the extended usage of SOCMINT. First, SOCMINT encourages what Omand et al. (2012: 804) call *"Crowd-sourced information"*. Social Media facilitates contributions of private citizens to aid authorities in critical situations and provide necessary information, which increases the amount of different sources. Second, Social Media provides law enforcement with the ability to detect unrest and criminal activity earlier through the availability of open-source data. Three additional advantages derive out of the improved understanding of movements through Social Media. Situational awareness of law enforcement, meaning the ability to detect crime situations and immediately respond to it, increases through the immediate availability of data and the augmented traffic on Social Media platforms after events or incidents, which facilitates the coordination of immediate reactions accordingly. This situational awareness results out of the additional sources and the additional data emerging via Social Media. The fourth advantage of SOCMINT is that authorities gain better insight into protest movement and groups and are therefore able to predict more exactly when protests with potential violent outbreaks take place. They can more easily observe reactions on certain events that are likely to cause extensive protests. The identification of criminal intents is described as the fifth advantage that occurs through SOCMINT, ameliorating possible preventions of criminal activities and further enabling predictive policing.

However, Omand et al. (2012: 806ff.) acknowledge challenges in the usage of SOCMINT. These lie mainly within the necessity and the legitimacy of using Social Media as means of intelligence. Omand et al. assess that it is crucial that authorities gain public acceptance for SOCMINT, which is achieved through proving necessity and legitimacy. *"In sum, intelligence activity must effectively contribute to a public good but not detract from or threaten any others in ways that are not recognized and appropriately managed"* (Omand et al. 2012: 807). Intelligence gathered from Social Media platforms needs to actively contribute to public safety and security and at the same time must not infringe upon the privacy of innocent citizens, which, given the enormous amount of data gathered from these platforms poses one major challenge: data needs to be reliable in order to aid intelligence operations and improve knowledge on defined issues. Due to the vast array of data, mistakes are more likely to happen, undermining legitimacy and effectiveness of SOCMINT. When Omand et al. (2012: 822) argue for a stronger inclusion of SOCMINT into intelligence and law enforcement, they acknowledge that *"[a]t the heart of this process are the twin demonstrations of necessity and legitimacy."*

Big Data, OSINT and SOCMINT are three concepts that are closely intertwined. While Big Data comprises the entity of the increasing amount of data, OSINT and SOCMINT describe special aspects of processed data, data that is used for intelligence purposes, therefore meaning data processed under certain assumptions. For policing, each of these developments poses major opportunities as well as challenges, which will be assessed in the following section.

4. Social Media and Policing Protests – Scholarly Debate and Practical Evidence

Social Media as a means of organizing protest has been a considerably big topic of discussion in scholarly debates (see Shirky 2011, Tufekci/ Wilson 2012, Fenton 2016). Research on the impact of Social Media on policing protests, however, remains underdeveloped and has just lately emerged as a topic of increased interest. However, in the course of the riots in Vancouver in 2011, London in 2011 and Ferguson in 2014, law enforcement's use of Social Media in detecting and controlling riots has evolved into a progressively vivid topic for scholars as well as responsible actors within law enforcement units. Trottier (2012: 415) argues that Social Media has led to an evolution in surveillance, with citizens actively contributing to surveillance by authorities, creating a bottom-up approach. On Social Media platforms, citizens actively contribute to creating networks and profiles, therefore rendering data more visible to law enforcement. Trottier describes his statement with the case study of the Hockey Riots in Vancouver in 2011, where two aspects of Social Media policing could be detected – direct communication and indirect data gathering. The first aspect describes the conscious offering of data to law enforcement such as names of rioters and locations where riots happened directly to police Social Media channels, the second aspect describes unconsciously making data available to police by posting Tweets[2] and uploading pictures publicly. Therefore Social Media, according to Trottier (2012: 422) will significantly change the policing of riots because of the vast amount of data that becomes easily available in a short period of time, by voluntary contributions as well as by status updates or uploaded photos that concern riots.. Police forces therefore will be able to more easily predict courses of protest movements and riots, thereby applying the concept of predictive policing on riot and protest policing. However, Trottier (2015: 542) also acknowledges that *"Social media uptake in OSINT by police remains in a formative stage"*. An interesting aspect of Trottier's analysis poses the perception that OSINT, and therefore SOCMINT, reconfigures Social Media platforms into public spaces. From a perspective of securitization, this development is central as Social Media as an arena of policing would signify a major securitizing move.

Panagiotopolous et al. (2014: 355) regard Social Media as an opportunity to increase communication between police and the public by improving information exchange. Informing the population on possible countermeasures and on safety developments has been facilitated enormously by Social Media. SOCMINT, in this regard, becomes a two-faced instrument – as law enforcement obtains information on protests and riots via Social Media, policing measures can be improved and more information for protecting public safety is available, which, in turn, can be shared via Social Media. This of course offers the opportunity for protesters and rioters to change their actions according to the data provided by law enforcement. SOCMINT therefore can also serve as a sort of *"protester intelligence"*, albeit in a very limited manner.

Joh (2014: 42) focuses on the influence Big Data has on policing processes; most prominently, Big Data is used for predictive policing, Joh assesses that attempting to predict crimes according to the analysis of data is *"[p]erhaps the most visible use of big data by police departments"*. However, as she states, Big Data also fosters computer enhanced mass surveillance (2014: 48). In the narrative of mass surveillance, due to the high number of people registered on Social Media platforms, surveillance of individuals has been greatly facilitated. While this rightfully causes numerous privacy concerns, police can make use of this gathered data to analyse interactions, movements and developments that could lead to riots, for example Tweets of escalating protests or people inciting violent acts via Facebook.

The analysis thus far shows that Big Data and Social Media are developing into increasingly important means of (predictive) policing; also the following examples from the United States and United Kingdom illustrate this. As data on the usage of Social Media for predicting and policing protests and riots is mainly classified, the analysis will be based on reports and official documents such as strategies and agendas.

Central for the analysis of US police forces is a report by the Department of Justice's Office of Community Oriented Policing Services (COPS), a subunit of the Department of Justice dedicated to improve community policing (COPS 2013), which contains a variety of important aspects of SOCMINT and policing. For example, the report suggests that police should monitor Social Media platforms closely in the organization of flash-mobs in order to effectively prevent these, therefore mitigating the risk of the flash-mob turning into a riot (COPS 2013: 22). In the case of policing protests and riots, Social Media becomes even more important in order to learn about protest movements and to develop the capability of shaping these (ibid: 30) The report also recognizes the need for capacities in order to be capable of coping with large amounts of data. The New York Police Department (NYPD) has created a specialized unit within its intelligence division with the task of monitoring Social Media networks in order to establish advanced warning for events that are likely to require police forces (ibid: 14), as did the Boston Police Department (BPD) in the course of the Occupy protests (Davis III et al. 2014: 12). The BPD used Social Media *"to monitor and engage with protesters so police could gauge the crowd's intent and adjust tactics in real time"* (ibid).

The influence of Social Media in the US on protests and policing became particularly vivid during the Ferguson riots in fall 2014. After the shooting of an African-American by a police officer, Tweets emerged that led to increased media interest and coverage, and as consequence of the disclosure of the killing, protests erupted (Freelon et al. 2016: 42). These protests turned out to become violent, even leading the governor of Missouri to proclaim the state of emergency. Social Media played a vital role in the formation of the protests, a report by COPS in the aftermath of the riots determined. *"Social media was the key global driver of the Ferguson demonstrations. It provided the virtually simultaneous communication channels that facilitated crowd building and crowd movement"* (COPS 2015). In the report, COPS assessed that law enforcement forces in Ferguson have failed to develop a viable Social Media strategy in order to cope with the information given during the protests.

---

2   Tweets are short public messages on Twitter.

According to the COPS report (2015: 97), more than three million tweets were posted on Ferguson, providing a nearly unmanageable amount of data. As the report discloses, the Saint Louis Police Department established a group to monitor Social Media activities within its Intelligence division, providing a practical case of SOCMINT during riots. Social Media was used *"to gauge the tenor of the protest"*, authorities however failed to successfully prevent violent outbreaks and guarantee public safety and order.

Similar observations can be made in the case of the aftermath of the 2011 riots in the United Kingdom. Williams et al. (2013: 466f.) assess that in the course of these riots, closed networks like messaging services were the dominant means of communication to organize protests, which made obtaining open-source data difficult. However, authorities admit that in some cases, open-source data on planned riots was available and aided in preventing a planned looting in London (HMIC 2011: 31). British authorities admitted after the 2011 riots that the power of Social Media was underestimated and it was necessary to improve capabilities to quickly analyse and effectively use the data obtained on these platforms. The HMIC[3] also elaborates the opportunity of using Social Media as means of intelligence but acknowledges the obstacle of the massive amount of data produced in these networks and the incapability of police forces to successfully handle this amount of data (ibid: 6). Therefore, the establishment of instruments such as a 'data-mining engine', a software that scans across publicly available social media for possible shifts in protest movements, possibly developing riots and other warning signals signal crimes was recommended (ibid: 39). The improved monitoring of Social Media should not only produce improved data understanding, but also make use of tools such as geo-coding, if users made their location available publicly, in order to attach possible movements to locations and improve situational awareness. Examining the findings and suggestions of the HMIC, the strategy poses a prime example for practical usage of SOCMINT, obstacles and advantages described in the strategy are similar to the findings as described by Omand et al. (2012) and objectives through SOCMINT are clearly defined in creating better situational awareness and improving the ability to react to protest movements quickly and accordingly.

5. Conclusion

This article explored two questions: Does the increased use of Big Data and especially Social Media lead to a securitization of these technologies? How has Social Media impacted the policing of protests? In terms of the first question, policing is regarded as a securitizing move, as it is a reaction to a perceived security threat – crime and riots, for example. Social Media prominently prove to be a security enabler in this context, as it assists and facilitates policing by providing data on possible internal security threats. Social Media as an arena of interactions that also comprise security threatening

issues becomes a security matter as such, and means of modern communication become increasingly securitized. As securitization is often shaped through discourses, SOCMINT as a means of policing will at least increase the perception of Social Media as a securitized issue. As outlined in the examples of protest policing, law enforcements spends considerable attention to Social Media as security enabler, which further points to a securitization process.

In terms of the second question, Big Data and Social Media prove viable instruments for the evolution of predictive policing. As the practical examples have shown, focus in protest policing is put rather on the early detection and possible prevention of protests than on the reaction. Predictive policing is therefore also increasingly visible in the policing of protests. In addition, Social Media and Big Data prove to represent important security enablers in this regard, as they ease the prediction of crime and riots. Therefore, I argue that through enabling and facilitating predictive policing, Social Media and Big Data have impacted policing, and I estimate the influence to grow within the coming years.

To conclude, I want to outline that research on the field of Social Media and internal security is still at the beginning. However, given the importance that law enforcement agencies devote to the inclusion of Social Media and Big Data into their strategies, research will gain more importance.

Clemens Binder (MA) is a researcher at the Austrian Institute of International Affairs (oiip) in the section of Science, Technology and International Relations. He studied Political Science in at the Universities Vienna and Oslo and holds a Master's degree from the University of Vienna. Clemens is specializing in the influence of technology and Big Data on security policy.

Literature

Bachner, Jennifer; Lynch, Jennifer (2016): Is Predictive Policing the Law-Enforcement Tactic of the Future? Wall Street Journal Online http://www.wsj.com/articles/is-predictive-policing-the-law-enforcement-tactic-of-the-future-1461550190 (retrieved August 15th, 2016)

Bijker, Wiebe (2001): Understanding Technological Culture through a Constructivist View of Science, Technology and Society. In: Cutliffe, Stephen; Mitcham, Carl (eds.):Visions of STS: Counterpoints in Science, Technology, and Society Studies, State University of New York Press, Albany, pp.19-34

Boyd, Danah, Crawford, K. (2012) Critical Questions for Big Data. Information, Communication & Society 15:5, 662-679

Brooks, David (2013): The Philosophy of Data. New York Times Onlinehttp://www.nytimes.com/2013/02/05/opinion/brooks-the-philosophy-of-data.html?_r=0 (retrieved August 18th, 2016)

Buzan, Barry, Wæver, Ole, de Wilde, Jaap(1998): Security. A new framework for Analysis. Rienner, Boulder

Ceyhan, Ayse (2008): Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. In: Surveillance & Society 5(2): 102-123

COPS (2013): Social Media and Tactical Considerations for Law Enforcement. Washington, D.C. http://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/social%20media%20and%20tactical%20considerations%20for%20law%20enforcement%202013.pdf (retrieved May 21st, 2016)

COPS(2015): After-Action Assessment of the Police Response to the August 2014 Demonstrations in Ferguson, Missouri. COPS Office Critical Response Initiative. Washington, DC: Office of Community Oriented Policing Services.

Couch, Neil/ Robins, Bill (2013): Big Data for Defence and Security. RUSI Occasional Paper

Cukier, Kenneth; Mayer-Schoenberger, Viktor (2013a): The Rise of Big Data. How It's Changing the Way We Think About the World. In: Foreign Affairs 92(3), pp. 28-40

Cukier, Kenneth; Mayer-Schoenberger, Viktor (2013b): Big Data. A Revolution That Will Transform How We Live, Work and Think. John Murray, London

Davis III, Edward; Alves, Alejandro; Sklansky, David (2014): Social Media and Police Leadership: Lessons from Boston. New Perspectives in Policing Bulletin, U.S. Department of Justice

---

3   Her Majesty's Inspectorate of the Constabulary (HMIC) is a British institute that assesses the work of police forces and formulates recommendations.

Earl, Jennifer/ Soule, Sarah A./ McCarthy, John D. (2003): Protest under Fire? Explaining the Policing of Protest. In: American Sociological Review 68(4), pp. 581-606

Fenton, Natalie (2016): Left out? Digital media, radical politics and social change. In: Information, Communication and Society 19(3), pp. 346-361

Freelon, Deen/ Mcilwain, Charlton/ Clark, Meredith (2016): Beyond the Hashtag. Ferguson, Black Lives Matter and the Struggle for Online Justice. Center for Media and Social Impact.http://archive.cmsimpact.org/sites/default/files/beyond_the_hashtags_2016.pdf (retrieved May 24th, 2016)

HM Government (2014): Emerging Technologies: Big Data. HM Government Horizon Scanning Programme https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/389095/Horizon_Scanning_-_Emerging_Technologies_Big_Data_report_1.pdf (retrieved August 15th, 2016)

HMIC (2011): The rules of engagement. A review of the August 2011 disorders. https://www.justiceinspectorates.gov.uk/hmic/media/a-review-of-the-august-2011-disorders-20111220.pdf (retrieved May 20th, 2016)

Joh, Elizabeth (2014): Policing by Numbers: Big Data and the Fourth Amendment. In: Washington Law Review 89(35), pp. 35-68

Lim, Kevjn (2016): Big Data and Strategic Intelligence. In: Intelligence and National Security 31(4), pp. 619-635

McPhail, Clark/ Schweingruber, David/ McCarthy, John (1998): Policing Protest in the United States: 1960-1995 In: della Porta, Donatella/ Reiter, Herbert (eds.): Policing Protest: The Control of Mass Demonstrations in Western Democracies. University of Minnesota Press, Minneapolis, pp. 49-69

Omand, Sir David/ Bartlett, Jamie/ Miller, Carl (2012): Introducing Social Media Intelligence (SOCMINT). In: Intelligence and National Security 27(6), pp. 801-823

Panagiotopolous, Panagiotis/ Bigdeli, Alinaghi Ziaee/ Sams, Steven (2014): Citizen-government collaboration on social media: The case of Twitter in the 2011 riots in England. In: Government Information Quaterly 31, pp. 349-357

Perry, Walter et al. (2013): Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. RAND Corporation

Scott, Len/ Jackson, Peter (2008): The Study of Intelligence in Theory and Practice. In: Johnson, Loch/ Wirtz, James (eds.): Intelligence and National Security. Oxford University Press, Oxford, pp. 21-37

Shirky, Clay (2011): The Political Power of Social Media. In: Foreign Affairs January/ February 2011

Trottier, Daniel (2012): Policing Social Media. In: Canadian Review of Sociology 49(4), pp. 411-425

Trottier, Daniel (2015): Open Source Intelligence, social media and law enforcement: Visions, constraints and critiques. In: European Journal of Cultural Studies 18(4-5), pp. 530-547

Tucker, Joshua (2014): Tweeting Ferguson: how social media can (and cannot) facilitate protest. Washington Post <https://www.washingtonpost.com/blogs/monkey-cage/wp/2014/11/25/tweeting-ferguson-how-social-media-can-and-can-not-facilitate-protest/"> (retrieved May 22nd, 2016)

Tufekci, Zeynep/ Wilson, Christopher (2012): Social Media and the Decision to Participate in Political Protest: Observations from Tahrir Square. In: Journal of Communication 62, pp. 363-379

Ulbricht, Lena; von Grafenstein, Maximilian (2016): Big Data: Big Power Shifts? In: Internet Policy Review 5:1

Wæver, Ole (1995): Securitization and Desecuritization. In: Lipschutz, Ronnie (ed.): On Security, Columbia University Press, New York, pp. 46-86

Williams, Matthew L. et al. (2013): Policing cyber-neighbourhoods: Tension monitoring and social media networks. In: Policing and Society 23(4), pp. 461-481

Williams, Michael (2003): Words, Images, Enemies: Securitization and International Politics. International Studies Quarterly 47, pp. 511-531