Article

The Surveillance Dimensions of the Use of Social Media by UK Police Forces

Elena M. Egawhary

Columbia University, USA
eme2151@columbia.edu

Abstract

This paper explores the various surveillance practices involved in the use of social media for communication and investigation purposes by UK police forces. In doing so, it analyses internal policy documents and official guidance obtained through freedom of information (FOI) requests sent to 46 police forces in the United Kingdom. This analysis finds that UK police forces advise their staff to simultaneously engage in both surveillance and counter-surveillance strategies in their use of social media as a policing tool.

Introduction

The use of social media by UK police forces falls into two broad categories: communication (or engagement) and investigation (or operational use). UK police forces began registering corporate accounts on Twitter and Facebook for communication purposes for the first time in 2008. However, UK police forces' use of the internet for investigative purposes dates back to April 2001 with the creation of the National Hi-Tech Crime Unit (NHTCU) to "investigate attacks on the Critical National Infrastructure; major internet based offences of paedophilia, fraud or extortion; information from seized electronic media and gather intelligence on cybercrime and cybercriminals" (Corbitt 2001: 29). Prior to 2001, most of the responsibility for using social networking sites to investigate crime fell to a small number of digital evidence recovery officers who were "swamped and learning on the job" (Thomas 2005) resulting in a reportedly "huge workload" (Goodwin 2005). This suggests that the use of social media in UK policing began in an unstructured way and "on the basis of initiatives by individual officers and subsequently with varying degrees of official support" (Crump 2011: 1). The increase in user-generated content, through the use of social networking sites in the early 2000s led to a shift in the nature of the internet from a repository of useful datasets and organisational websites to a source of highly detailed real-time personal information. The London Riots, in August 2011, were a pivotal moment in the investigative use of social media platforms for UK police forces as it "simultaneously highlighted both the enormous potential value of digital communications in controlling crime and disturbance and the UK police's ill-preparedness for such analysis" (Edwards and Urquhart 2016: 280). The result is that police forces in the UK have been increasingly moving away from viewing the internet (and social media) as being solely the domain of either communication departments or specialized investigators; instead, they view online space as simply another beat to police.

Methodology and limitations

There are 45 territorial police services in the United Kingdom as well as a number of special police forces, one of which is included in this paper. Each police force is led by a chief constable who is “operationally independent” (NPCC 2019). This paper relies on internal policy documents and official guidance obtained through freedom of information (FOI) requests sent to 46 police forces in the UK. Of these 46 police forces, 72 percent provided policy documents in relation to the use of social media as a communication tool and 59 percent disclosed policy details surrounding the use of social media for investigative purposes.

While freedom of information requests as a form of “coercive institutionalized discovery practice” (Marx 1984: 78) can have “great potential on both theoretical and practical levels” (Savage and Hyde 2014: 304), their limitations have also been noted. Due to their multi-faceted nature, “there is nothing straightforward about FOI as a law or social research method” (Luscombe and Walby 2017: 384). FOI regimes are “subject to systemic and endemic flaws” (Walby and Larsen 2011: 39) with much of the data released being subject to all sorts of possible mediation. It is difficult to know if what has been provided is fully representative or accurate, whether key information has been destroyed, missing or excluded, or whether a response has been shaped in a particular way by the responding institution. Furthermore, FOI requests can be blunt instruments. Unless researchers resort to a protracted and costly legal process, they must accept what is provided and in this sense be a relatively passive actors in the research process. This has certainly been true in the research process for this paper, whereby certain forces have stated that they are in a period of transition when it comes to policy guidance in both the communication and investigation spheres.

Nonetheless, there is value to be had in utilising FOIs to obtain information that might not be otherwise available. FOI requests can provide a “partial entrance into a little known realm of texts” (Walby and Larsen 2011: 39) that would otherwise never form part of the public record. Even in situations where information has been redacted or a researcher is denied open opportunities to examine what a police force has deemed too sensitive to disclose to members of the public FOI requests provide an opportunity to consider why such information is restricted.

A final limitation to consider is that policy guidance within the policing context has rarely been found to be the basis of police action. Police officers have been found to pay “little to no attention to policy manuals and administrative rules” (Luscombe and Walby 2017). In addition, there are a number of other sources of information that would determine practice in this area, such as training courses for officers operating in this area. Nonetheless, this paper does not seek to detail actual practice nor to claim that police practice in this area is solely or wholly based on the information that has been obtained. That would be too much to ask of static documents. Rather what is sought is an understanding of the perception of the surveillance affordances of social media at an organisational level in UK policing as described in the documents that have been provided.

Surveillance Practices by UK Police Forces in their Use of Social Media

An examination of internal policy documents finds that they discuss five surveillance affordances of social media: general surveillance of the local community, encouraging the local community to surveil each other, managerial surveillance, peer-to-peer surveillance, and surveillance in pursuit of an investigative aim. The first four forms of surveillance are to be found in policy guidance relating to the use of social media as a communication tool; the fifth use is outlined in policy documents relating to the use of social media within an investigative context. It should be noted, however, that guidance on the use of social media for communication purposes varies considerably by police force. For example, Merseyside Police and West Midlands Police expressly prohibit all “surveillance or monitoring work” (Merseyside Police 2013: 11; West Midlands Police 2014: 6) without proper authority.

General Surveillance of the Local Community for Communication Purposes

Fourteen forces mention the potential to monitor the online population they interact with so as to “assess sentiment” (British Transport Police 2017: 2) and engage in “environmental scanning” (Police Service of Northern Ireland 2017: 1). The aim is to pick up any “emerging community issues” (Police Service of Northern Ireland 2017: 5) or “wider national issues” (Wiltshire Police 2014: 7). Indeed Greater Manchester Police argues that “monitoring social networking sites allow us to build intelligence and identify any potential issues that can arise” (Greater Manchester Police 2014: 7). Although sentiment analysis and the sorting of the local population in the context of policing protests was found to be “a marginal aspect of police social media practices” (Dencik, Hintz, and Carey 2018: 1443), categorisation is being used in the communication departments of some police forces. Devon and Cornwall Police explain, in their FOI response, that Facebook advertising is used for PR, campaigns, and recruitment purposes to specifically target people in Devon and Cornwall and that “adverts can be targeted to geographic locations and by demographic information (age, gender etc.) which provides a highly targeted communication tool” (Devon and Cornwall Police 2018: 1) particularly as “Facebook also provides detailed statistics for each advert which are evaluated and reviewed after each campaign” (Devon and Cornwall Police 2018: 1). The difference between targeted advertisements in specific hard copy publications and targeted advertisements via social media platforms such as Facebook, however, is the opportunity for the non-targeted audience to view such advertisements: on social media, only the targeted audience will see the advertisement. Social media campaigns, whether targeted or not, have led some forces to expend significant sums of money. When Essex Police shifted its use of Facebook from boosting operational posts to using Facebook adverts for recruitment and safety campaigns their yearly expenditure on Facebook was almost nine times higher, a shift from £5,860.22 in 2016 to £46,325.54 in 2017 (Essex Police 2018).

Engaging the Local Community to Surveil Each Other

Twenty police forces promoted social media as a communication tool as a way of “involving people in policing” (Warwickshire Police and West Mercia Police 2016: 2). Engaging with the local community on social media provides an opportunity to “seek information, intelligence and evidence” (Thames Valley Police 2017: 18) from “often hard-to-reach audiences that may not engage with traditional media” (Wiltshire Police 2014: 7). This is an area where the boundary between communication and investigative work is not clear but rather where “there may be some cross over between operational and non-operational use” (Devon and Cornwall Police 2016: 2).

Managerial Surveillance

Twenty-six forces informed staff members that if they set up a professional social media account for communication purposes, then they will be monitored to ensure their posts are appropriate. This monitoring can take place in a number of departments or units within each police force. Usually such oversight is undertaken by media and corporate communication departments (Norfolk Constabulary and Suffolk Constabulary 2017: 9); however, sometimes heads of units are given this responsibility (Cheshire Constabulary 2017: 4), as well as professional standards departments (Merseyside Police 2013: 2). In some policy documents, officers and staff are warned that failure to act in accordance with the policy “may amount to a misconduct or criminal offence and will be referred to the Professional Standards Branch for assessment” (Greater Manchester Police 2014: 6). Such cases have come to fruition with police officers losing their jobs not only over their use of official accounts but also for posting “offensive messages” (Philipson 2014) on personal or anonymous social media accounts (Telegraph Reporters 2016).

Some policies provide staff with examples of posts that are unacceptable due to poor grammar or spelling, information that is in contempt of court, or the use jargon or “police speak” (Hertfordshire Constabulary 2018: 3). Police officers and staff are advised not to post restricted or sensitive information, not to imply that an individual is guilty of a crime, not to post operational material, and not to “post anything that you wouldn’t say in front of a member of the public or the Chief” (Durham Constabulary 2015: 2). Gloucestershire Constabulary include a real-world example of an “inappropriate and insensitive

message”¹ tweeted by the official Merseyside Police Twitter account referencing rape that weakened “the confidence that the public have in the police—especially victims of this particular crime” (Gloucestershire Constabulary 2017: 4).

Positive examples of posts are also provided as a form of guidance. Officers and staff are told to write short and snappy posts, to use pictures and hashtags where appropriate, to report local good news, positive policing news, and crime prevention advice (Durham Constabulary 2015: 2). An undated presentation document provided by Humberside Police includes good example messages, such as a post linking to a press release about the introduction of body worn cameras stating: “Body worn cameras – helping bring domestic abuse offenders to justice. Domestic abuse is our number one priority” (Humberside Police n.d.: 6).

The extent of the monitoring varies, with some police forces using free online tools, such as Tweetdeck or Hootsuite (Police Service of Northern Ireland 2017: 5) whilst others rely on corporate software, such as CrowdControlHQ which provides “omni-visual” (Wiltshire Police 2014: 18) dataveillance of their staff’s use of corporate social media accounts. Police officers and staff engaging on social media on behalf of the police force are not solely monitored on the basis of what they write but in some cases on the basis of how often they write and how successfully they engage with their target audience. Northamptonshire Police inform staff that “News & Publishing will monitor approved accounts for inactivity” (Northamptonshire Police 2016: 10). Thus where accounts are approved, there is an expectation that they will “be regularly used” (Bedfordshire Police 2018: 5). Hertfordshire Constabulary’s guidelines advise that “as a minimum, five tweets should be posted per week” (Hertfordshire Constabulary 2018: 1). Officers who request to operate a corporate social media account at Dyfed-Powys Police must agree to supply monthly feedback to the Corporate Communications department about how their account successfully engaged with their target audience (Dyfed-Powys Police 2018: 5).

Whereas historically it has been argued that police culture is “obdurate” (Ericson and Haggerty 1997: 33) when faced with new technology—in this case, where police officers and staff are assigned a corporate social media account which they must update regularly—the technology appears to have “altered institutional police practices in a manner consistent with the logic of social media platforms” (Schneider 2016: 123).

Peer-to-Peer Workplace Surveillance

Four police forces encourage peer-to-peer workplace surveillance in the context of social media activity. Officers and staff are urged to “report, challenge or take action” (Cumbria Constabulary 2018: 2) if their colleagues do anything they think might be inappropriate on a social media account. One force goes further than merely suggesting, telling its staff that “this is a clear direction that you have a duty to report matters that offend against the standards of professional behaviour both offline and online” (Cumbria Constabulary 2018). The Press Association reported that, between January 2009 and February 2014, fully 828 police employees were “investigated for breaching social media guidelines at forces across England and Wales” (Press Association 2014).

Surveillance in Pursuit of an Investigative Aim

Police force policy and guidance in relation to the use of the internet (including social media) for an investigative purpose is more consistent across forces than it is for communication purposes. Twenty-one forces disclosed a redacted copy of guidelines, dated 2015, which were developed by the National Open Source Intelligence Working Group at the National Police Chiefs’ Council (NPCC). The NPCC is a body that brings together a majority of the UK’s chief police officers in an attempt to drive improvement and coordinate operations and reform. This 2015 NPCC guidance was “approved nationally to define the levels of activity for Open Source Intelligence” (National Police Chiefs’ Council 2015: 9). However,

¹ <https://www.gloucestershire.police.uk/media/5518/2017-09-force-social-media-policy.pdf> [accessed March 23, 2019].

Avon and Somerset Constabulary provided a more recent document entitled NPCC Internet, Intelligence & Investigations Strategy, dated 2018. At the time of writing, the NPCC was shifting its guidance for online investigation and intelligence work from the 2015 model to the new 2018 model.

The 2018 guidance is also the only policy relating to the use of social media for investigative purposes that was provided unredacted. The reasons given for redaction or refusal, in all other cases, pointed to concerns that knowledge of how investigative work is carried out on social media platforms could lead to “catastrophic damage” (British Transport Police 2018) as it “would provide those with the necessary intent the knowledge of our capabilities in this field which would likely lead to them taking steps to amend how they use such platforms” (Metropolitan Police Service 2018).

The NPCC 2015 Guidance (The Five-level Model)

The NPCC 2015 guidance refers to five levels of activity for Open Source Intelligence and Research, with the first three levels described as being “open source intelligence/research” (National Police Chiefs’ Council 2015: 9) and the final two levels being redacted in their entirety. Despite these redactions, Her Majesty’s Inspectorate of Constabulary (HMIC) in 2014 published a document distinguishing among what it calls “levels of undercover online investigations” (Her Majesty’s Inspectorate of Constabulary 2014: 200) in Annex F of the report *An Inspection of Undercover Policing in England and Wales*. It is unclear whether these levels are precisely the same levels as those partially redacted in the 2015 NPCC guidance; however, it is notable that the unredacted wording of Levels 1 to 3 in the 2015 NPCC Guidance at pages 9 to 10² almost exactly matches the wording of the first three levels outlined in Annex F of the HMIC report at pages 200 to 201.³

The five-level model (at times, with minor changes) is referred to and relied upon in a number of other specific police force policies and, on occasion, simplified further into categories (Cleveland Police 2018: 4). The Police Service of Scotland (Police Scotland), for example, does not use the NPCC guidance but instead references three “tiers” in its internet research and investigations standard operating procedures (Police Scotland 2018: 6).

Under the five-level model, level 1 refers to overt internet investigatory work such as searching social media sides and other publicly available websites overtly. Examples include checking whether an individual has a social media account and viewing public profiles to secure evidence or intelligence.

Levels 2 and 3 refer to online research that is covert, namely when the subject is unaware they are being surveilled. Examples include the use of fake profiles to log onto Social Networking sites. There must be no interaction at this level, “no befriending subjects, poking, writing on walls or joining groups” (Her Majesty’s Inspectorate of Constabulary 2014: 200). When operating at this level police officers must work on “non-attributable computers” (Her Majesty’s Inspectorate of Constabulary 2014: 200) or “covert internet workstations” (Metropolitan Police Service 2014: 8) whereby no electronic “footprint” is left and the IP address is not connected to the Police Force itself. Any information that is recovered as a result of Level 2 or 3 research must be recorded in the Force Intelligence Management system. Any fake personas created to allow officers to access social media sites must be registered in the Force fake persona record (Her Majesty’s Inspectorate of Constabulary 2014: 200). Officers are also likely to require authorisation to undertake “directed surveillance” under section 28 of the Regulation of Investigatory Powers Act 2000 (RIPA).

The purpose of RIPA is “to provide a comprehensive regulatory structure governing the interception of

²https://www.suffolk.police.uk/sites/suffolk/files/003525-16_npcc_guidance_redacted.pdf [accessed March 23, 2019].

³<https://www.justiceinspectors.gov.uk/hmicfrs/wp-content/uploads/an-inspection-of-undercover-policing-in-england-and-wales.pdf> [accessed March 23, 2019].

communications, access to communications data, covert surveillance, the use of informants and other covert human intelligence sources, and the decryption of encrypted material” (Cape 2008: 239). The Act “lays down the purposes for which different techniques may be deployed” (Clarke 2001: 35) and how oversight will be conducted.

Levels 4 and 5 involve elements of covert interaction online. Level 4 involves an officer making contact with a subject through the “use of passive profiles with limited interaction” (Her Majesty’s Inspectorate of Constabulary 2014: 201). Level 5 on the other hand involves interaction whereby an officer establishes or maintains a personal or other relationship with a person online for the covert purpose of obtaining information. Level 5 requires not only further training in the form of a nationally accredited Foundation Undercover Officer online course but also Covert Human Intelligence Source (CHIS) authorisation under RIPA section 29. CHIS authorisation requires that necessity and proportionality have been demonstrated, but it also has additional criteria which must be met prior to authorisation; specific arrangements must be made to ensure that the source is independently managed and supervised, that records are kept of the use of the source and that the source’s identity is protected from those who do not need to know it. Both Level 4 and Level 5 research must be carried out on non-attributable computers with special consideration given to ISP and IP matching. In addition officers are advised to seek support in both cases from a disclosure officer “to assist in the protection of tactics through parallel sourcing of material obtained and PII [Public Interest Immunity] applications” (Her Majesty’s Inspectorate of Constabulary 2014: 201).

Under the five-level model it becomes clear that with each increased level of surveillance there is supposed to be increased training for officers and greater oversight from internal mechanisms, such as requiring authorisation under RIPA. As well as increased oversight, police officers also intensify their counter surveillance practices with each increased level of surveillance they undertake, such as the use of non-attributable computers and disclosure officer support. Nonetheless, there is a degree of overlap between levels and at times poorly defined distinctions.

The NPCC 2018 Guidance (The Capability Delivery Model)

On April 30, 2018, the NPCC Internet Intelligence and Investigations Portfolio produced details of a capability delivery model (see Figure 1) in order to provide greater “clarity around training requirements and authorisation of covert activity online...with a simple and straight forward framework” (National Police Chiefs’ Council 2018: 5).

**Note - Covert Internet Intelligence & Investigations does not include authorised Undercover Online (UCOL). This activity falls under the remit of the UC Capability Lead.*

Figure 1: The Capability Delivery Model as outlined on page 6 of the NPCC Internet Intelligence & Investigations Strategy

Under the capability delivery model, activities that constitute undercover policing and would require covert human intelligence source (CHIS) authorisation under the Regulation of Investigatory Powers Act 2000 (RIPA) (see Level 5 on page 201 in the HMIC Report⁴) have been entirely removed from the realm of internet intelligence and investigations and would fall under the remit of undercover policing.

Under the capability delivery model there are three levels of activity: core internet use; overt internet intelligence and investigations; and covert internet intelligence and investigations.

Core internet use is described as “the overt and ad hoc use of online resources and search engines to provide basic information” (National Police Chiefs’ Council 2018: 6). Examples cited include capturing online evidence highlighted by a witness; accessing online mapping facilities in preparation for what is termed “executive action” (National Police Chiefs’ Council 2018: 6); and utilising online data sources such as 192.com, an online public record database, and Companies House, the UK’s corporate registry. The key distinguishing factor is that officers operating under the category “core internet use” must “not access areas of the internet which require a username and password” (National Police Chiefs’ Council 2018: 6). All officers and staff will be provided with internet safety training to conduct this level of work in a way that “does not exceed their remit or risk compromise” (National Police Chiefs’ Council 2018: 6).

Overt internet intelligence and investigations is described as “a structured, methodical, task driven and planned approach to online research, conducted by a suitably trained (and current) individual” (National Police Chiefs’ Council 2018: 7). Examples of the type of work that can be undertaken under this category include using overt profiles to log into and access platforms, using advanced search techniques to conduct systematic and focused research, monitoring online activity in relation to pre-planned and spontaneous events, and capturing intelligence and evidence in support of an ongoing investigation (National Police Chiefs’ Council 2018: 7). The key distinguishing factor for this category of online investigative work is that no covert tactics are to be used; and where a username and password are required to access an online space, the credentials provided must reflect the fact that the account or profile is being used for a policing purpose and a record of all activity conducted must be kept. No activity conducted as overt internet intelligence and investigations should require authority under RIPA or any other covert authority. Systematic monitoring of a personal profile (even when it is open and an overt police account is being used) is considered to be activity that would fall within covert internet intelligence and investigations. This is because it is considered to be a form of “directed surveillance” under section 28 of RIPA and, as such, would require a directed surveillance authority (DSA), under the Act, prior to being carried out so as to ensure that such surveillance is both proportionate and necessary. Finally, it is stipulated that restrictions on corporate web browsers and the technical implications of a fixed IP address may mean that overt searches will need to be conducted using internet connectivity outside of the normal Police network and infrastructure.

Covert internet intelligence and investigations is also described as “a structured, methodical, task driven and planned approach” (National Police Chiefs’ Council 2018: 7). Activities outlined as falling under this category of online investigative work include facilitating covert access to closed and private groups and areas, covertly gathering evidence and intelligence, conducting online surveillance of a known subject or group and facilitating the deployment of additional online covert tactics. This category of investigative work will only be conducted by personnel who are suitably trained and have been expressly authorised by the relevant force or agency. Furthermore, and mirroring the language of RIPA, covert internet intelligence and investigations tactics are stipulated to “only be utilised after all other reasonable, less intrusive, methods have been considered and it is proportionate and justified to do so” (National Police Chiefs’ Council 2018: 8). This type of investigative work will always require a directed surveillance authority (DSA) or other covert authority. In circumstances where an authority is deemed not to be

⁴<https://www.justiceinspectors.gov.uk/hmicfrs/wp-content/uploads/an-inspection-of-undercover-policing-in-england-and-wales.pdf> [accessed March 23, 2019].

needed, it is stated that the rationale for this decision must be recorded. Individuals conducting this work will routinely use “covert accounts or profiles, obfuscated internet connections and suitable hardware” (National Police Chiefs’ Council 2018: 8). They are instructed that they must not use force or agency networked computers unless they are using an “appropriate portal solution” (National Police Chiefs’ Council 2018: 9) that makes use of independent internet connectivity and virtualisation techniques.

The 2018 model shifts the focus of online investigative work away from the nature of the information that is to be found online and instead focusses on how the police have captured the data; namely, on police conduct. Thus, how open or available online information becomes is less important than how the police collect, analyse, and store it. In both the 2015 and 2018 NPCC guides, however, it is clear that when the internet and, as such, social media are used for investigative purposes, there is also an increased training requirement for officers at each increased level of surveillance, the need for greater oversight from internal mechanisms such as requiring authorisations under RIPA (although it should be noted that the effectiveness of such oversight can at times be flawed [Office of Surveillance Commissioners 2017: 18]) and, finally, with each increased level of surveillance, counter-surveillance practices must also be intensified such as in avoiding the use of police networked computers with identifiable IP addresses and using covert accounts and profiles.

UK Police Forces’ Use of Social Media in their Counter-Surveillance Practices

Some of the policy documents, both in terms of communications guidance and online investigation and intelligence guidance, allude to the ability for social media to “augment the visibility of police work” (Trottier 2012: 147) and caution staff about a number of surveillance risks, namely sousveillance from the general public, surveillance by the media, or surveillance by criminals or legal teams, legal and regulatory oversight, and technological surveillance.

Sousveillance by the General Public

The guidance of twenty-three forces highlights the increased public visibility of the police force and its officers. Staff are informed that social media has given members of the public “a tremendous voice to raise awareness and hold organisations and individuals to account” (Cheshire Constabulary 2017: 3); they are also reminded of the importance of professional conduct online as well as offline. Some policies also stipulate that anything posted in private on corporate social media accounts, such as direct messages, can still be requested under the Freedom of Information Act (West Yorkshire Police 2014: 12).

Surveillance by the Media

Twenty-one forces warn their staff that their “accounts will be followed by members of the media as well as members of the public” (Northamptonshire Police 2016: 13) who “constantly monitor Facebook and Twitter” (Hertfordshire Constabulary 2018: 2) to “use social media to gather information about policing” (Norfolk Constabulary and Suffolk Constabulary 2017: 7). Warnings to officers include checking “who someone is before responding” (Cheshire Constabulary 2017: 5) as the individual may be a journalist or a blogger. Some forces go further and warn that the media “quite often ‘follow’ or make ‘friends’ with officers” (Greater Manchester Police 2014: 5) to gather information about individuals such as “personal details, telephone numbers, email addresses and links, images and interests which can be used to discredit officers and staff” (Hampshire Constabulary 2015: 5). Certain policy documents warn staff to be vigilant of “social engineering attacks” (Hampshire Constabulary 2015: 3) whereby they might be manipulated into disclosing information or carrying out certain actions. In short, guidance documents advise staff and officers that on social media platforms “people will be actively searching for your mistakes, including the media” (Wiltshire Police 2014: 6) but that they “should not fight against this scrutiny...but...accept it as an important characteristic of modern society” (Wiltshire Police 2014: 9).

Surveillance by Criminals or Legal Teams

Fourteen forces advise staff and officers that they should not link their personal lives or personal social media accounts to their professional lives or professional social media accounts in case they are monitored by “criminals who wish to gain your trust and then take advantage of that trust for criminal purposes” (Norfolk Constabulary and Suffolk Constabulary 2017: 14). They also warn police officers that “serious and organised criminals and terrorists have been found to use social networking sites to identify targets for subversion, blackmail or attack” (Devon and Cornwall Police 2016: 7) and, when monitoring their social media, to be wary of individuals wishing to cause them, their family, or their friends harm. Some forces warn that not only criminals but also legal teams may be monitoring police officers and staff on social media: “legal teams representing external parties can use social media to gather information about individuals...which can be used to discredit officers and staff” (Hampshire Constabulary 2015: 5). The latest strategy document from the NPCC stipulates that “in order to protect the privacy and safety of officers and staff, and their family, as well as maintaining evidential and professional integrity, social media and internet accounts used for policing purposes must be separated from those used for personal social networking” (National Police Chiefs’ Council 2018: 10).

Legal and Regulatory Surveillance

The policy documents often detail the legal framework for the use of social media as an investigative tool, in particular, the obligations under RIPA, defamation law, human rights legislation, copyright law and disclosure rules. However, advice and discussion of the laws surrounding social media use and other regulatory frameworks is inconsistent, with some forces providing detailed guidance and others simply referring to the legislation in passing.

Technological Surveillance

The guidance documents touch upon, in varying degrees of detail, the manifold ways in which social media and electronic equipment are used to surveil officers. These include the dangers associated with the geolocation functionalities of social media apps and devices (Northamptonshire Police 2016: 14); the risks of third party unknown apps (West Midlands Police 2014: 8); the insecurity and susceptibility to viruses or hacking attempts of not only physical devices but also social media platforms; and the surveillance implications of posting photographs to social media websites (Derbyshire Constabulary 2012: 6). Officers are also warned that using a computer connected to the Police National Network risks an individual being informed that someone from the static IP address connected to the police force was examining their profile or website, namely the leaving of an electronic footprint (Police Scotland 2018: 5; Metropolitan Police Service 2014: 8). Devon and Cornwall Police emphasise to staff that “an electronic footprint is everlasting” (Devon and Cornwall Police 2016: 7).

Kent Police warn staff that Internet Service Providers maintain a record of IP addresses and the sites visited as well as the fact that individual websites may record IP addresses or other details and may also install cookies that can track their online activity (Kent Police 2018: 4). The NPCC are even more specific in warning that providers of websites and applications can and will record the IP addresses of those using their services and that whilst this is usually not a threat to law enforcement:

Less scrupulous website providers may use this information to identify Law Enforcement Officers who are conducting enquiries on overt Police computers. Where this activity is for a lawful policing purpose and no security has been overcome or falsehood used to enter a site this should not limit our investigations. (National Police Chiefs’ Council 2018: 10)

Conclusion

Through an analysis of policy documents produced by UK police forces regarding the use of social media as a communication tool and an investigation tool, this paper has attempted to elucidate some of the ways

in which police forces at an organisational level perceive the opportunities to surveil the population they serve through the use of social media as well as their perceptions of how their officers and staff might be surveilled in turn. There is certainly room for further research in this area in order to draw a more fulsome history of how social media usage became interwoven with policing practice in the UK. Though this attempt to sketch an initial surveillant assemblage (Haggerty and Ericson 2000) cannot be said to demonstrate actual police practice or present a complete picture, it does provide an idea of the level of cognisance social media surveillance affords at an administrative level in UK police forces and that, at times, this can be vague, inconsistent, and incomplete between forces. Such an analysis also provides an opportunity to see what may have been omitted from UK police forces' guidance to their staff. For example, it is striking that there is no mention of the ability of social media companies to surveil police forces and their interactions with members of the public. The concern about corporate surveillance is limited to the informational security of platforms in regard to hackers rather than the platforms themselves, and whether or how they might make economic use of their intermediary position between the police and the public.

References

- Alex Luscombe, and Kevin Walby. 2017. Theorizing Freedom of Information: The Live Archive, Obfuscation and Actor-Network Theory. *Government Information Quarterly* 34: 379–87.
- Bedfordshire Police. 2018. *Bedfordshire Police: Social Media Policy*. <https://www.bedfordshire.police.uk/assets/Beds-FOI/FOI-2018/September-2018/FOI201804542-AnnexA.pdf>
- British Transport Police. 2017. *Social Media Strategy 2017/18*. Retrieved at <http://btpa.police.uk/publications/policing-plans/national/>
- British Transport Police. 2018. *FOI Response: 1376-18*.
- Cape, Ed. 2013. Regulation of Investigatory Powers Act 2000. In *Dictionary of Policing*, edited by Tim Newburn and Peter Neyroud, 238-239. Abingdon, UK: Routledge.
- Cheshire Constabulary. 2017. *Social Media Procedure Reference: 2015/07*. <https://www.cheshire.police.uk/contact/social-media-accounts/social-media-guidance/>
- Clarke, Charles. 2001. The Role of Legislation and Regulation of Investigatory Powers Act. *The RUSI Journal* 146 (3): 35–37.
- Cleveland Police. 2018. *North East Regional Special Operations Unit Research of Open Source Material and Social Networking Sites Guidance*.
- Corbitt, Terry. 2001. National Hi-Tech Crime Unit. *Management Services*, February 2001.
- Crump, Jeremy. 2011. What Are the Police Doing on Twitter? Social Media, the Police and the Public. *Policy & Internet* 3 (4).
- Cumbria Constabulary. 2018. *Online Code of Conduct*. <https://www.cumbria.police.uk/Information-Rights/Policy-Documents/Conduct-of-Police-Force-Business/Online-Code-of-Conduct-Final.pdf>
- Dencik, Lina, Arne Hintz, and Zoe Carey. 2018. Prediction, Pre-Emption and Limits to Dissent: Social Media and Big Data Uses for Policing Protests in the United Kingdom. *New Media & Society* 20 (4): 1433–50.
- Derbyshire Constabulary. 2012. *Guidance on the Safe Use of the Internet and Social Media by Police Officers and Police Staff 09/268*. <http://www.derbyshire.police.uk/Documents/About-Us/Freedom-of-Information/Policies/SafeUseoftheInternetandSocialMediaByPoliceOfficersandPoliceStaffGuidance.pdf>.
- Devon and Cornwall Police. 2016. *Force Policy & Procedure: Use of Social Media D256*. <https://www.devon-cornwall.police.uk/FOI/Doc/c08efaa3-ed96-4581-83ce-384049905918/p?D256%20open.pdf>
- Devon and Cornwall Police. 2018. *FOI Request: 0442/18*.
- Durham Constabulary. 2015. *Durham Constabulary Policy*. <https://www.durham.police.uk/About-Us/.../Limited%20Duties%20Policy%20V2.pdf>
- Dyfed-Powys Police. 2018. *Corporate Communications Social Media Guidance*. <https://www.dyfed-powys.police.uk/en/about-us/our-departments/corporate-communications/>
- Edwards, Lillian, and Lachlan Urquhart. 2016. Privacy in Public Spaces What Expectation of Privacy Do We Have in Social Media Intelligence? *International Journal of Law and Information Technology* 24 (3): 279–310.
- Ericson, Richard V., and Kevin D. Haggerty. 1997. *Policing the Risk Society*. Toronto: University of Toronto Press.
- Essex Police. 2018. *FOI Request 26/11/2018*.
- Gloucestershire Constabulary. 2017. *Social Media Policy*. <https://www.gloucestershire.police.uk/media/5518/2017-09-force-social-media-policy.pdf>
- Goodwin, Bill. 2005. Police Forced to Turn Away E-Crime Victims. *Computer Weekly*, April 12, 2005.
- Greater Manchester Police. 2014. *Media and Social Media Communications: Policy & Procedure*.
- Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51 (4): 605–22.
- Hampshire Constabulary. 2015. *33501 Procedure - Digital Engagement & Personal Use of Social Media*. https://www.hampshire.police.uk/SysSiteAssets/foi-media/hampshire-constabulary/policies/33501_procedure_-_digital_engagement_and_personal_use_of_social_media.pdf.

- Her Majesty's Inspectorate of Constabulary. 2014. *An Inspection of Undercover Policing in England and Wales*. <https://www.justiceinspectors.gov.uk/hmicfrs/wp-content/uploads/an-inspection-of-undercover-policing-in-england-and-wales.pdf>
- Hertfordshire Constabulary. 2018. *Protocol for Use of Social Media*. <https://www.herts.police.uk/assets/FOI-Herts/FOI-2018/September-2018/FOI201804550-Sep2018AnnexeB.pdf>.
- Humberside Police. n.d. *Hello and Welcome Presentation*.
- Kent Police. 2018. *S2800 Policy - Open Source and Social Media*. <https://www.essex.police.uk/getmedia/c8d5d717-30f6-411f-a417-c886a1e86b70/S2800-Policy-Open-Source-and-Social-Media.pdf>.
- Marx, Gary T. 1984. Notes on the Discovery, Collection and Assessment of Hidden and Dirty Data. In *Studies in the Sociology of Social Problems*, edited by Joseph W. Schneider and John I. Kitsuse, 78-113. New Jersey: Ablex Publishing Corporation.
- Merseyside Police. 2013. *Digital & Social Media (Policy & Procedure)*. <https://www.gov.uk/government/publications/social-media-guidance-for-civil-servants/social-media-guidance-for-civil-servants>
- Metropolitan Police Service. 2014. *Internet & Social Media Use in the MPS: Guidance*.
- Metropolitan Police Service. 2018. *FOI Response: 2018100000303*.
- National Police Chiefs' Council. 2015. *NPCC Guidance on Open Source Investigation/Research*.
- National Police Chiefs' Council. 2018. *Internet Intelligence & Investigations Strategy*.
- National Police Chiefs' Council. 2019. *National Police Chiefs' Council Website*. January 5, 2019. <https://www.npcc.police.uk/About/QuestionsandAnswers.aspx>
- Norfolk Constabulary, and Suffolk Constabulary. 2017. *Digital and Social Media Policy*.
- Northamptonshire Police. 2016. *Social Media Policy*.
- Office of Surveillance Commissioners. 2017. *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2016-2017*. HC 299 SG/2017/222.
- Philipson, Alice. 2014. Police Officer Sacked over Twitter Account Which Called Force Bosses 'Scum.' *The Telegraph*, April 4, 2014. <https://www.telegraph.co.uk/news/uknews/law-and-order/10765037/Police-officer-sacked-over-Twitter-account-which-called-force-bosses-scum.html>
- Police Scotland. 2018. *Internet, Research and Investigations: Standard Operating Procedures*. <http://www.scotland.police.uk/assets/pdf/151934/184779/internet-research-and-investigations-SOP>
- Police Service of Northern Ireland. 2017. *Corporate Policy Service Instruction SI1017 Social Media*.
- Press Association. 2014. Hundreds of Police Staff Investigated over Use of Facebook and Twitter. *The Guardian*, August 18, 2014. <https://www.theguardian.com/uk-news/2014/aug/19/police-facebook>
- Savage, Ashley, and Richard Hyde. 2014. Using Freedom of Information Requests to Facilitate Research. *International Journal of Social Research Methodology* 17 (3): 303-17.
- Schneider, Christopher J. 2016. *Policing and Social Media: Social Control in an Era of New Media*. Lanham, MD: Lexington Books.
- Telegraph Reporters. 2016. Policeman Sacked after He Uses Twitter to Call for Benefits Street Estate to Be 'Bulldozed with People Still Inside.' *The Telegraph*, August 15, 2016. <https://www.telegraph.co.uk/news/2016/08/15/policeman-sacked-after-he-uses-twitter-to-call-for-benefits-stre/>
- Thames Valley Police. 2017. *Electronic Communications Policy*.
- Thomas, Daniel. 2005. Security—Specialist Police Units Tackle Computer Crime. In Their Fourth Year, Hi-Tech Crime Units Are Proving Invaluable to Police Forces across the Country. *Computing*, October 13, 2005. <https://www.computing.co.uk/ctg/feature/1834395/specialist-police-units-tackle-crime>
- Trottier, Daniel. 2012. *Social Media as Surveillance: Rethinking Visibility in a Converging World*. Farnham, UK: Ashgate.
- Walby, Kevin, and Mike Larsen. 2011. Access to Information and Freedom of Information Requests: Neglected Means of Data Production in the Social Sciences. *Qualitative Inquiry* 18 (1): 31-42.
- Warwickshire Police, and West Mercia Police. 2016. *Social Media Policy*. [https://www.warwickshire.police.uk/media/1086/Social-Media-Policy-Harmonised/pdf/Social_Media_Policy_\(Harmonised\).pdf](https://www.warwickshire.police.uk/media/1086/Social-Media-Policy-Harmonised/pdf/Social_Media_Policy_(Harmonised).pdf)
- West Midlands Police. 2014. *Social and Digital Media Policy CC/01*. http://foi.west-midlands.police.uk/wp-content/uploads/2014/05/Social_and_Digital_Media.pdf.
- West Yorkshire Police. 2014. *Force Web and Social Media Sites Policy*. https://www.westyorkshire.police.uk/sites/default/files/force_web_and_social_media_sites.pdf.
- Wiltshire Police. 2014. *Social Media Guidance: A Guide for Police Officers and Police Staff*. https://www.wiltshire.police.uk/media/467/Social-Media-Guidance/pdf/Social_Media_Guidance.pdf?m=636469590469170000.

Appendix 1.

A geographic representation of the areas of operation of UK police forces who were sent FOI requests for this paper.

Appendix 2.

The policy documents that were disclosed under FOI are listed below. Please note this is not an exhaustive list of all policy documents relating to social media use by UK police forces, simply those that were disclosed to the author and relied upon for this paper.

POLICE FORCE	COMMUNICATION POLICY	INVESTIGATION POLICY
Avon and Somerset Constabulary	Guidelines on the Safe use of the Internet and Social Media by Police Officers and Police Staff ACPO 2013	Redacted Copy of NPCC Internet Intelligence & Investigations Strategy 2018 v1
	Engage: Digital and Social Media Engagement for the Police Service NPJA	
	College of Policing Authorised Professional Practice (APP) for Engagement and Communication.	
Bedfordshire Police	Bedfordshire Police: Social Media Policy	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
British Transport Police	Social media strategy 2017/18	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
Cambridgeshire Constabulary	Not Provided	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
Cheshire Constabulary	Cheshire Constabulary Social Media Procedure Reference 2015/07	Not Provided
City of London Police	Not Provided	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
		Redacted Copy of Force Policy & Standard Operating Procedure Open Source Intelligence 2017
Cleveland Police	Not Provided	Redacted Copy of North East Regional Special Operations Unit Research of Open Source Material and Social Networking Sites v1.2 2018
Cumbria Constabulary	Cumbria Constabulary Online Code of Conduct	Not Provided
Derbyshire Constabulary	Derbyshire Constabulary Guidance on the Safe Use of the Internet and Social Media by Police Officers and Police Staff Policy Reference 09/268	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
Devon and Cornwall Police	Devon & Cornwall Police Use of Social Media D256	Not Provided
Dorset Police	Not Provided	Not Provided
Durham Constabulary	Durham Constabulary Social Media Policy 2015	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
Dyfed-Powys Police	Dyfed-Powys Corporate Communications Social Media Guidance	How to Capture Audio and Video Files Sent Using Facebook Messenger (a guide)
	Dyfed-Powys Corporate Communications Social Media Strategy 17-18	Downloading your Twitter Archive
Essex Police	Not Provided	Not Provided
Gloucestershire Constabulary	Gloucestershire Constabulary Social Media Policy	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
Greater Manchester Police	Greater Manchester Police Media and Social Media Communications Policy & Procedure May 2014	Not Provided

POLICE FORCE	COMMUNICATION POLICY	INVESTIGATION POLICY
Gwent Police	Not Provided	Not Provided
Hampshire Constabulary	Hampshire Constabulary 33500 Policy - Use of Social Media	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
	Hampshire Constabulary 33501 Procedure - Digital	
	Engagement & Persona Use of Social Media	
	Protocol for use of social media	
Humberside Police	Social Media Training Presentation October 2017	Not Provided
Kent Police	Not Provided	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
		Redacted Copy of S 2800 Policy - Open Source and Social Media
		Redacted Copy of S 2801 Procedure/SOP - Open Source and Social Media
Lancashire Constabulary	Not Provided	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
Leicestershire Police	Leicestershire Police Social Media Policy 2016	Not Provided
Lincolnshire Police	Lincolnshire Police Policy Document 2017 Social Media PD 174(6)	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
Merseyside Police	Merseyside Police Digital & Social Media (Policy & Procedure) 2013	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
	Guidelines on the Safe use of the Internet and Social Media by Police Officers and Police Staff ACPO 2013	
Metropolitan Police Service	Not Provided	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
		Redacted copy of Internet & Social Media Use in the MPS: Guidance document Version 1.6
Norfolk Constabulary	Norfolk & Suffolk Constabulary 2017 Digital and Social Media 41	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
		Redacted Copy of Norfolk Constabulary and Suffolk Constabulary Cyber Investigation and Open Source Intelligence Research 160 2017
North Wales Police	North Wales Police Online Social Networking Policy 2015 114	Extract of Online Social Networking Guidelines relating to investigative use
North Yorkshire Police	Not Provided	Redacted Copy of Open Source Research Procedure 120917 v1.2
Northamptonshire Police	Northamptonshire Police Social Media Policy January 2016 Rev. 5	Not Provided
Northumbria Police	Online Communication and Engagement via Forums, Blogs and Social Media 2016	Extract of Procedure entitled 'Crime Investigation'
Nottinghamshire Police	Nottinghamshire Police Social and Digital Media Policy Version 1.4 February 2017	Not Provided

POLICE FORCE	COMMUNICATION POLICY	INVESTIGATION POLICY
Police Scotland	Not Provided	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
		Redacted Copy of Manual of Guidance on Internet Investigations 2013
		Redacted Copy of Internet, Research and Investigations Standard Operating Procedures 2018
Police Service of Northern Ireland	Corporate Policy Service Instruction SI1017 Social Media 2017	Not Provided
South Wales Police	Not Provided	Not Provided
South Yorkshire Police	Engagement and Communication Reference P6	Not Provided
	Social and Digital Media for Engagement Instructions Reference Pi6.3	
Staffordshire Police	Social Media - Legal Dos and Don'ts	Not Provided
	Social Media - Management of Content	
	Social Media - Monitoring of Content	
	Social Media - Setting up a Social Media Account	
	Social Media Policy	
Suffolk Constabulary	Norfolk & Suffolk Constabulary 2017 Digital and Social Media 41	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
		Redacted Copy of Norfolk Constabulary and Suffolk Constabulary Cyber Investigation and Open Source Intelligence Research 160 2017
Surrey Police	Social Media Process Flow Chart	Not Provided
Sussex Police	Not Provided	Not Provided
Thames Valley Police	Thames Valley Police Electronic Communications Policy 2017 3.2	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
Warwickshire Police	Warwickshire Police and West Mercia Police Media Communications Policy v1.1 Nov16	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
	Social Media Guidance: a guide to effective social media use	Warwickshire Police and West Mercia Police Open Source Investigation Policy A007 V2.0
	Warwickshire Police and West Mercia Police Social Media Policy v1.1 Sep 16	
West Mercia Police	Warwickshire Police and West Mercia Police Media Communications Policy v1.1 Nov16	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
	Social Media Guidance: a guide to effective social media use	Warwickshire Police and West Mercia Police Open Source Investigation Policy A007 V2.0
	Warwickshire Police and West Mercia Police Social Media Policy v1.1 Sep 16	
West Midlands Police	West Midlands Police Social and Digital Media Policy CC/01	Redacted Copy of NPCC Guidance on Open Source Investigation/Research 2015
West Yorkshire Police	West Yorkshire Police Force web and social media sites	Not Provided

POLICE FORCE	COMMUNICATION POLICY	INVESTIGATION POLICY
Wiltshire Police	Wiltshire Police Social Media Guidance A guide for police officers and police staff	Not Provided
	Wiltshire Police Social Media Policy 2016 v2.0	
	Our Social Media Code of Conduct	
	Staying safe on social media	