



21 May 2020

Sir Brian Leveson
IPCO
PO Box 29105
London
SW1V 1ZU

via email: info@ipco.org.uk

Dear Sir Leveson,

RE: Social media monitoring by local authorities: regulatory issues

We enclose a copy of our report "Is your Local Authority looking at your Facebook likes?" ("the Report").

We are concerned that a significant number of Local Authorities carry out overt social media monitoring (understood as looking at publicly available data on social media and where privacy settings are available but not applied)¹ in a range of areas, including debt recovery, regulatory services, anti-fraud, children's social care and protest monitoring, without comprehensive guidance or internal oversight.

Our research builds on observations made by the Office of Surveillance Commissioners (OSC) as early as 2014,² echoed nearly every year thereafter,³ that some local authorities used social media for investigative purposes.

In order to assess the breadth of this practice across Local Authorities, in October 2019 we sent Freedom of Information requests (under the Freedom of Information Act 2000 and the

¹ This definition is consistent with the definition provided by the Office of Surveillance Commissioners set out at *Oversight arrangements for covert surveillance and property interference conducted by public authorities and to the activities of relevant sources* (July 2016) ('The Oversight Arrangements'), para. 289.1, available at: <https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf>

² OSC, *Annual Report for 2013-2014* (September 2014), available at: <https://www.ipco.org.uk/docs/OSC%20Annual%20Report%202013-14.pdf.pdf>

³ Privacy International, *History of the UK Regulators' concerns regarding Local Authority use of social media monitoring*, available at: <https://privacyinternational.org/long-read/3531/history-uk-regulators-concerns-regarding-local-authority-use-social-media-monitoring>



Freedom of Information (Scotland) Act 2002) to every Local Authority in Great Britain (251 recipients). We analysed 136 responses, all of which were received in November 2019. These Local Authority responses are publicly available for consultation.⁴

Based on our research, 62.5% of all responsive Local Authorities admitted to carrying out overt social media monitoring. In summary, their shared understanding was that the absence of privacy settings meant that the data could be considered open source and was therefore viewable without authorisation when consulted on a “one-off” basis, a denomination which is open to wide interpretation. Consequently, “one-off” viewings are largely unrecorded, unsupervised and unregulated. Such revelations are concerning.

Increased interest by Local Authorities in using social media in investigations

Some Local Authorities noted in their responses that the use of social media investigations had become commonplace. Others highlighted the opportunity offered by social media to obtain highly detailed information about a person and their activities, noting its usefulness in investigating alleged offences with a view to bringing a prosecution.

Local Authorities also revealed using overt social media monitoring in a range of areas, including debt recovery, regulatory services, anti-fraud, children’s social care and protest monitoring. Concrete instances of social media monitoring in these areas are referenced in the Report.

Use of privacy settings as an indicator of the lawfulness of viewing

Our research showed that only 53.7 % of Local Authorities who carried out overt social media monitoring had an accompanying policy.⁵ The position of Local Authorities as to what social media material could be freely accessed was homogenous: where privacy settings were not applied by the user, the information could be considered open source or publicly available. This conclusion is based on guidance issued by the OSC in 2016 (the 2016 Guidance), which

⁴ WhatDoTheyKnow, *Social Media Monitoring – a batch request*, available at: https://www.whatdotheyknow.com/info_request_batch/858

⁵ Privacy International, *Methodology: Social Media Monitoring by UK Local Authorities*, available at: <https://privacyinternational.org/report/3530/methodology-social-media-monitoring-uk-local-authorities>



stated that social media users had a reasonable expectation of privacy where access controls were applied.⁶ Conversely, where such access controls were available and not applied, the data on social media could be considered open source. The guidance therefore implied that in those circumstances, users did not have a reasonable expectation of privacy – and was read accordingly by Local Authorities.

This approach mistakenly presumes that publicity of content ousts any privacy considerations. Extensive jurisprudence has confirmed that interactions in a public context may fall within the scope of the right to private life.⁷ Given that some content posted on social media would not have been voluntarily shared with a Local Authority, the question whether a reasonable expectation of privacy exists in relation to that content bears further consideration. If answered negatively, the resulting approach would place an onerous burden on users to be constantly vigilant of their privacy settings across social media platforms over time.

Unclear distinction between overt and covert social media monitoring

Another common feature among Local Authority policies was a distinction between “one-off” viewings – considered to be overt social media monitoring – and “repetitive examination” of public posts, which was considered to amount to covert social media monitoring that may be classed as directed surveillance.

In practice, this distinction is far from clear: the continued viewing of a profile over an extended period of time albeit in one sitting may arguably fall within the “one-off” category. Similarly, repetitive examination is so loosely defined that it is difficult to say with any certainty that two viewings or more will require, as a matter of necessity, further authorisation.

In any event, the distinction between overt and covert social media monitoring is rendered meaningless without a proper record of each viewing. Indeed, it is difficult to know whether the “repetitive examination” threshold has been reached in relation to an individual under

⁶ The Oversight Arrangements, available at: <https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf>
⁷ European Court of Human Rights, *Peck v United Kingdom*, para. 57.



investigation without a record of who viewed the individual's social media profile, when, and for how long.

Lack of internal oversight processes

The Report found that the majority of responsive Local Authorities conducting overt social media monitoring do not monitor or audit this practice internally. The absence of oversight and audits is concerning for a number of reasons. First, this means that Local Authorities are not in a position to assess whether viewings of social media profiles were erroneously categorised as "one-offs" and in hindsight would have amounted to directed surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA). Second, Local Authorities cannot assess whether overt social monitoring as an institutional practice is effective, or indeed whether the monitoring was necessary and proportionate. Third, Local Authorities are thus not in a position to ensure these practices are compatible with the European Convention on Human Rights in accordance with section 6 of the Human Rights Act 1998. Finally, whilst not within the IPCO's remit, given that this monitoring of social media may involve the processing of personal data, it raises questions about Local Authorities' ability to comply with data protection obligations, including 'accountability', the requirement to be responsible for, and be able to demonstrate compliance with the data protection principles.

The absence of a necessity and proportionality assessment

Local Authorities are not satisfying any criteria prior to undertaking overt social media monitoring. Whilst RIPA requires directed surveillance to satisfy criteria of necessity and proportionality prior to being authorised (RIPA s.28), no such imperative appears to exist in relation to overt social media monitoring.

However, in circumstances where the absence of internal audits and oversight mechanisms signify that the effectiveness of social media monitoring remains an open question, Privacy International stresses that any social media monitoring exercise should be subjected to internal assessments of (i) whether the data is sought in pursuance of a legitimate aim, (ii) whether the data is necessary for that legitimate purpose, and (iii) whether the social media monitoring is proportionate to what is sought to be achieved.



The impact of previous OSC/IPCO guidance

The matter of social media monitoring by Local Authorities has been previously addressed by the IPCO itself, and its predecessor, the OSC, on multiple occasions. However, both the OSC and IPCO have largely focussed on directed surveillance activities and their compliance with RIPA, excluding detailed consideration of overt social media monitoring. Where guidance has addressed the viewing of open source social media data, it has done so somewhat confusingly and inconsistently.

In the OSC 2015 annual report (the 2015 OSC Report),⁸ the Commissioner stressed that “just because material is out in the open, does not render it fair game”. However, the 2016 Guidance left it open for Local Authorities to conclude that the absence of privacy settings in a social media profile meant that users had no reasonable expectation of privacy despite extensive jurisprudence suggesting otherwise.⁹ The 2015 OSC Report stressed the need for oversight in relation to the access to social networking sites. However, the 2016 Guidance established oversight mechanisms only in relation to covert surveillance of social media profiles, which it did not comprehensively distinguish from overt social media monitoring. The 2016 Guidance neither imposes obligations on nor offers recommendations to Local Authorities regarding the approach they should take when contemplating overt social media investigations.

Ultimately, Local Authorities are left to grapple with the distinction between overt and covert social media monitoring – and there is no indication that they will err on the side of caution.

The impact of the Home Office Code of Practice

The Home Office published a revised Code of Practice on Covert Surveillance and Property Interference in 2018 ('the Code of Practice'). The Code of Practice notes, correctly, that privacy implications may attach to public social media content regardless of whether a user has applied privacy settings given that the intention when making such information available was

⁸ OSC, *Annual Report for 2014-2015*, available at: <https://www.ipco.org.uk/docs/OSC%20Annual%20Report%202014-15.pdf>

⁹ See fn.7.



not for it to be used for an investigative activity.¹⁰ In the following paragraph, however, the Code of Practice states that individuals posting information on social media networks are less likely to hold a reasonable expectation of privacy in relation to that information.¹¹

Once again, the information given to Local Authorities lends itself to multiple and inconsistent interpretations.

Recommendation

The Report shows that overt social media monitoring is proliferating among Local Authorities in the absence of clear guidance as to its limits or best practices. To the extent that social media monitoring activities are likely to expand in the future and for the reasons set out above, the need for you to review the position is important and urgent.

Specifically, we call on the IPCO to develop and publish guidance, with concrete examples, by reference to which Local Authorities may assess:

- What constitutes a legitimate aim for Local Authorities to rely on in order to conduct overt social media monitoring;
- In what circumstances overt social media monitoring is proportionate to these legitimate aims; and
- In what cases accessing publicly available social media content may result in directed surveillance

We look forward to hearing from you. If you require any further information from us, please do not hesitate to request it.

Yours sincerely,

Laura Lazaro Cabrera
Legal Officer
Privacy International

¹⁰ Home Office, Code of Practice on Covert Surveillance and Property Interference (August 2018), para. 3.13.

Available at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

¹¹ Ibid., para 3.14.