Is your Local Authority looking at your Facebook likes?

May 2020

privacyinternational.org

When Local Authorities aren't your Friends.

Is your Local Authority looking at your Facebook likes? Just because it's in the open, doesn't make it fair game.

It is common for families with no recourse to public funds who attempt to access support from local authorities to have their social media monitored as part of a 'Child in Need' assessment.

This practice appears to be part of a proactive strategy on the part of local authorities to discredit vulnerable families in order to refuse support. In our experience, information on social media accounts is often wildly misinterpreted by local authorities who make serious and unfounded allegations against our clients.

In some cases, local authorities will go so far as to use such information to make accusations of fraud and withhold urgently needed support from families who are living in extreme poverty.

This practice often leaves families too afraid to pursue their request for support, which puts them at greater risk of destitution, exploitation, and abuse.

Eve Dickson, Project 17

Table of Contents

When Local Authorities aren't your Friends. 1

Is your Local Authority looking at your Facebook likes? 1

Just because it's in the open, doesn't make it fair game. 1

SUMMARY 3

INTRODUCTION 6

Social media monitoring 6

Privacy Settings 7

What is repeated viewing 8

Accountability and legitimacy 10

Data integrity 10

Reframing social media platforms, users and data in terms of intelligence gathering and criminality 11

The future 12

FINDINGS 14

ANALYSIS OF FINDINGS 15

1. A significant number of local authorities are now using 'overt' social media monitoring and this substantially out-paces the use of 'covert' social media monitoring 15

2. If you don't have good privacy settings, your data is fair game for overt social media monitoring. 17

3. There is no quality check on the effectiveness of this form of surveillance on decision making 20

4. Your social media profile could be used by a Local Authority, without your knowledge or awareness, in a wide variety of their functions, predominantly intelligence gathering and investigations. 24

RECOMMENDATIONS 29

History of the regulators' concerns 30

Home Office Covert Surveillance and Property Interference Code of Practice, August 2018 38

ANNEX A: FOIA 42

SUMMARY

UK Local Authorities (local government) are looking at people's social media accounts, such as Facebook, as part of their intelligence gathering and investigation tactics in areas such as council tax payments, children's services, benefits and monitoring protests and demonstrations.

In some cases, local authorities will go so far as to use such information to make accusations of fraud and withhold urgently needed support from families who are living in extreme poverty.

Since 2011, the UK Chief Surveillance Commissioner[1], the regulator responsible for oversight of surveillance powers used by local authorities, has raised concerns about local authorities using the internet as a surveillance tool[2]. By 2017, such was the concern that Lord Judge wrote to every local authority suggesting that they conduct an internal audit of the use of social media sites and the internet for investigative purposes[3].

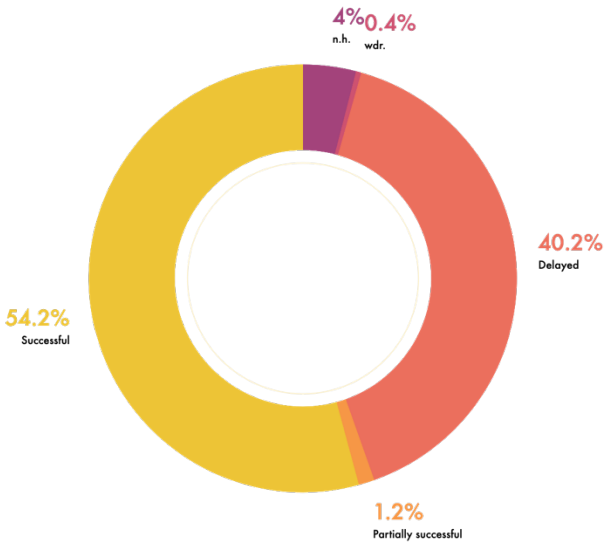
In October 2019 Privacy International sent a Freedom of Information Act request to every Local Authority in Great Britain (251 recipients) in relation to their use of social media monitoring. We asked not only about whether they had conducted an audit in response to Lord Judge's letter but sought to uncover the extent to which 'overt' social media monitoring in particular was being used and for what local authority functions.

The Surveillance Commissioner's Guidance[4] defines overt social media monitoring as looking at 'open source' data, being publicly available data and data where privacy settings are available but not applied. However, to be 'overt' it must also involve only a 'one-off' look at the individual's social media. If this becomes 'repeated viewing', even of so-called open source sites, then this becomes 'covert' social media monitoring.

We have analysed 136 responses to our Freedom of Information requests, being those that had been received by November 2019. All responses are publicly available on WhatDoTheyKnow.com. In this report, we chose to include excerpts from the responses we received to better illustrate the use of these practices.

[1] Replaced by the Investigatory Powers Commissioner in September 2017
[2] Privacy International, History of the UK Regulators' concerns regarding Local Authority use of social media monitoring: https://privacyinternational.org/long-read/3531/history-uk-regulators-concerns-regarding-local-authority-use-social-media-monitoring
[3] Office of Surveillance Commissioners, Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2015-2016: https://www.ipco.org.uk/docs/OSC Annual Report 2015-16.pdf
[4] Privacy International, Office of Surveillance Commissioners Guidance - Covert surveillance of Social Networking Sites (SNS): https://privacyinternational.org/long-read/3537/office-surveillance-commissioners-guidance-covert-surveillance-social-networking

Overall participation (Nov 2019)



	Successful	Delayed	Information not held (n.h.)	Partially successful	Withdrawn (wdr.)
Numbers of LA's	136	101	10	3	1
Percentual (Total = all LA's)	54.2%	40.2%	4%	1.2%	0.4%

Number of successful submissions
136

Our investigation has found that:

- A significant number of local authorities are now using 'overt' social media monitoring as part of their intelligence gathering and investigation activities. This substantially out-paces the use of 'covert' social media monitoring

- If you don't have good privacy settings, your data is fair game for overt social media monitoring.

- There is no quality check on the effectiveness of this form of surveillance on decision making.

- Your social media profile could be used by a Local Authority, without your knowledge or awareness, in a wide variety of their functions, predominantly intelligence gathering and investigations.

INTRODUCTION

Social media platforms are a vast trove of information about individuals, including their personal preferences, political and religious views, physical and mental health and the identity of their friends and families.

This wealth of information has attracted the interest of local authorities[5] who are increasingly checking Facebook and other social media accounts. They are using this for investigations and intelligence gathering in areas such as children's social care, council tax, fraud, licensing, benefits, neighbourhood services and debt recovery.

> Perhaps more than ever, public authorities now make use of the wide availability of details about individuals, groups or locations that are provided on social networking sites and a myriad of other means of open communication between people using the Internet and their mobile communication devices.
>
> Chief Surveillance Commissioner, The Rt Hon Sir Christopher Rose. Annual Report 2014-15

Social media monitoring

Social media monitoring refers to the techniques and technologies that allow the monitoring and gathering of information on social media platforms such as Facebook and Twitter.

The information can involve person-to-person, person-to-group, group-to-group and includes interactions that are private and public. For the purposes of 'overt' social media monitoring, this involves information such as messages and images that are posted publicly.

Whilst it is also possible to use certain tools to obtain data generated when you use a social media platform, such as location data or time of posting (i.e. meta data), it is not clear the extent to which local authorities can and do collect this data as part of 'overt' social media monitoring. Most local authorities currently search social media platforms manually.

As set out in Cheshire West and Chester Social Media Investigation and Review Policy, some of the sites that Local Authorities are likely to look at include Facebook, Twitter, YouTube, Snapchat, Instagram and Pinterest.

[5] See: Privacy International campaign "Neighbourhood Watched" on the use of intrusive technologies used by law enforcement: https://privacyinternational.org/neighbourhood-watched

> "Social Networking Sites (SNS) enable individuals, businesses and organisations to easily communicate with each other on a real time basis. Millions of users interact on these sites every day meaning that there is a vast amount of information recorded about users and their day to day lives.
>
> Social media can be very diverse, but will often have some, or all of the following characteristics; **The ability to show a list of other users with whom they share a connection; often termed "friends" or "followers"; The ability to view and browse their list of connections and those made by others within the system; Hosting capabilities allowing users to post audio, photographs and/or video content that is viewable by others; Social media can include community-based web sites, online discussion forums, chatrooms and other social spaces online as well.**
>
> For the purposes of this policy, examples of SNS include: Facebook, Twitter, YouTube, Tumblr, Flickr, Snapchat, Instagram, LinkedIn, Pinterest, Google+"

Privacy Settings

We are concerned that the respect given to an individual's privacy by local authorities in Great Britain, in relation to what individuals' say and do online, appears to be based on the arbitrary distinction of privacy settings. This distinction is supported by the Home Office guidance[6] and by the Regulator (the Investigatory Powers Commissioner[7]) whose annual reports document concerns related to local authority use of social media monitoring[8].

This is in a context where privacy settings constantly change and can apply differently to different content and situations, individuals may share without necessarily being aware who can access their information and how it is used.

> … contrary to popular belief, control of what data about you is public on social media is not simply a matter of easy voluntary choice. Accordingly, the common retort – if you didn't want people to read it, why did you make it public? – is not in fact a sensible

[6] Privacy International, Home Office Covert Surveillance and Property Interference, August 2018: https://privacyinternational.org/long-read/3532/home-office-covert-surveillance-and-property-interference-august-2018

[7] Privacy International, History of the UK Regulators' concerns regarding Local Authority use of social media monitoring: https://privacyinternational.org/long-read/3531/history-uk-regulators-concerns-regarding-local-authority-use-social-media-monitoring

[8] Privacy International, Office of Surveillance Commissioners Guidance - Covert surveillance of Social Networking Sites (SNS): https://privacyinternational.org/long-read/3537/office-surveillance-commissioners-guidance-covert-surveillance-social-networking

> question to ask. We would argue this contributes strongly to an argument that material placed on "open" social media can still carry with it reasonable expectations of privacy.
>
> Lilian Edwards and Lachlan Urquhart, 'Privacy in Public Spaces: What Expectations of Privacy do we have in Social Media Intelligence

To elaborate, if you don't know how to check your privacy settings or use social media platforms that have no settings, your information will be treated as 'open source' and local authorities can look at it, (as they state in response to our Freedom of Information Requests) for 'intelligence gathering' and 'investigations', without you ever knowing.

By contrast, where individuals have strict privacy settings and use platforms that offer controls, these individuals are granted 'a reasonable expectation of privacy' in relation to their social media posts and not subject to the same intrusion.

> Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. The fact that an individual is not told about "surveillance" does not make it covert. Notice the words in the definition of covert; "unaware that it is or maybe taking place." If an Officer decides to browse a suspect's public blog, website or "open" Facebook page, this will not be regarded as covert."
>
> Blaenau Gwent Country Borough Council Guidance

What is repeated viewing

Further, it is only when this form of surveillance is said to involve repeated viewing of an individual's social media that authorisation is required. The Investigatory Powers Commissioner has advised that repeat viewing of a suspect's profile on "open sources" sites may constitute directed surveillance and require a higher level of authorisation (known as RIPA authorisation[9]).

[9] RIPA is the law governing the use of covert techniques by public authorities. It requires that when public authorities, such as local authorities, need to use cover techniques to obtain private information about someone, they do it in a way that is necessary, proportionate, and compatible with human rights. RIPA's guidelines and codes apply to actions including covert social media monitoring. Local authorities in the UK have a wide range of functions and are responsible in law for enforcing over 100 separate Act of Parliament. In particular local authorities investigate in the following areas: trading standards, environmental health, benefit fraud. As part of their investigation a local authority may consider that it is appropriate to use a RIPA technique to obtain evidence. From 1 November 2012 local authorities are required to obtain judicial approval prior to using covert techniques. https://www.gov.uk/guidance/surveillance-and-counter-terrorism
RIPA use requires the internal approval of an Authorising Officer but also that of a magistrate.

> Casual (one-off) examination of public posts on social networks as part of investigations undertaken is allowable with no additional RIPA consideration. Repetitive examination/monitoring of public posts as part of an investigation must be subject to assessment and may be classed as Directed Surveillance as defined by RIPA.
>
> Arun District Council Guidance on the Use of Social Media in Investigations

Yet there is a lack of consistency as to what constitutes repeat viewing. From the Freedom of Information responses, we have received and the policies some local authorities have disclosed[10] with these responses, it appears that if a local authority spent time looking at an individual's social media, kept that page open, took screenshots[11] of the page and stored those, this may be 'overt' and does not require authorisation or result in any checks and balances.

Blackburn with Darwen Borough Council's procedural guide, for example, states that spending over three weeks googling or otherwise monitoring a person's name on various dates during that time may not fall within the Regulation of Investigatory Powers Act [RIPA[12]], although it would require use of their non-RIPA form. Other local authorities refer to 'one-off searches' of social media.

> 17. Non –RIPA forms are likely to be required if the proposed activity does not fall within RIPA but can be considered to be likely to breach a person's right to respect for his private and family life. So if you are going to spend over three weeks googling or otherwise monitoring a person's name on various dates during that time then that should trigger a NON RIPA form at the very least. It may depend upon how many hits you may click on during those weeks and the type of information uncovered. Consider whether what you

[10] These are available on the platform whatdotheyknow.com
https://www.whatdotheyknow.com/info_request_batch/858

[11] Cheshire West and Chester:
"The following relates to the accessing of publicly available SNS data only:
… Once content available from an individual's Social Media profile has been identified as being relevant to the investigation being undertaken, it needs to be recorded and captured for the purposes of producing as evidence. Depending on the nature of the evidence, there are a number of ways this may be done. Where evidence takes the form of a readable or otherwise observable content, such as text, status updates or photographs, it is acceptable for this to be **copied directly from the site, or captured via a screenshot, onto a hard drive or some other form of secure storage device, and subsequently printed to a hard copy**. Where evidence takes the form of audio or video content, then efforts should be made to **download that content** onto a hard drive or some other form of storage device such as a CD or DVD. When capturing evidence from an individual's public Social Media profile, steps should be taken to ensure that all relevant aspects of that evidence are recorded effectively. For example **taking a screenshot of a person's Social Media profile**, the Council officer doing so shall make sure that the time and date are visible on the screenshot in order to prove when the evidence was captured."

[12] RIPA is an Act of the UK Parliament regulating the powers of public bodies to carry out surveillance and investigation, and covering the interception of communications.

> are seeing really is intended to be 'open source' even if you do find it on an open source site.
>
> Blackburn with Darwen Borough Council, Procedural Guide for the use of covert surveillance and covert human intelligence sources

Lincoln City Council states that two visits are acceptable before it amounts to Directed Surveillance.

> "It is considered proportionate to visit a Social Media sites where there are no privacy settings twice in connection with an investigation (for example benefit fraud) but any further visits could amount to Directed Surveillance and require RIPA authorisation."
>
> Lincoln City Council

Accountability and legitimacy

Whilst this approach, which results in different exploitation of individuals' social media is approved by the Investigatory Powers Commissioner[13], the regulator who oversees use of surveillance powers by public authorities in the United Kingdom, there has been a notable absence of public and parliamentary debate. Key questions such as the legitimate aim of such activities and whether social media monitoring is necessary and proportionate in the different contexts it is being deployed by local authorities, have not been debated publicly, nor appear to have been considered at a local level in sufficient detail.

In most cases classed as 'overt' social media monitoring, there is rarely any form of authorisation and there is an absence of audit and accountability.

Data integrity

We are concerned that not enough consideration has been given to the inherent lack of data integrity, authenticity, veracity or the social context of conversations that may take place on social media. Leading to potential misinterpretation and reliance upon misleading 'evidence'.

[13] Office of Surveillance Commissioners Procedures and Guidance, July 2016 states "289.1 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied…Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis, and this should be borne in mind."

> "Social media have been discursively framed as a kind of public sphere, and there are a range of limitations to this ideal, including issues of privatisation, categorical discrimination and unequal access. Yet public spaces are historically ephemeral, as any social actor's engagement and disengagement with that space is relatively frictionless. Furthermore, the social actor can be present and visible in a public space while protected by the guise of relative anonymity. As an ideal, the outburst in the public square or the incendiary letter to the editor does not have an absolute bearing on the social standing of its author. Yet folding social media into open sources furthers the potentiality that the former are simultaneously a kind of public sphere and public record."[14]
>
> Daniel Trottier, European Journal of Cultural Studies

Making judgments based on social media is plagued by problems of interpretation. What does it mean when you 'like' or share a post on Facebook? Are you endorsing it, raising awareness, or opposing it? What intelligence can be gained from who you interact with and the photos you post.

> Obtaining evidence through the use of social media is often the most useful tool but requires particular care.
>
> Swindon Borough Council

Reframing social media platforms, users and data in terms of intelligence gathering and criminality

We live in an age where our communications and interactions with individuals, friends, organisations, governments and political groups take place on social media. It has provided an opportunity for the instantaneous transfer and publication of our identities, views, interactions, and emotions. The growing intrusion by government authorities' risks impacting what people say online[15], leading to self-censorship, with the potential deleterious effect on free speech, and other fundamental rights.[16] We have seen the way it is already being used to

[14] Daniel Trottier, European Journal of Cultural Studies 2015, Vol.18(4-5) 530-547
[15] See Privacy International campaign "When social media makes you a target": https://privacyinternational.org/when-social-media-makes-you-target
[16] For more information refer to Privacy International's archive of examples of abuse resulting from the use of social media monitoring: https://privacyinternational.org/examples/social-media-surveillance-socmint

monitor recipients of welfare benefits,[17] as part of immigration enforcement mechanisms[18] as well as to crack down on civil society.[19]

We may have nothing to hide, but if we know our local authority is looking at our Facebook, we are likely to self-censor. The impact is a reframing of social media platforms, users and data in terms of intelligence gathering and criminality.

> …any new proposals for intelligence gathering in an internet age will raise issues over access to personal data and their use by the state, as well as broader concerns about the effect surveillance work might have on the economic and social value of the internet as a place of free exchange of ideas and information. [20]
>
> #Intelligence, DEMOS, Sir David Omand, Jamie Bartlett, Carl Miller

Whilst we may be living much of our lives onto social media sites, we provide information, however innocuous, that we are unlikely to share with local authorities when asked directly, unless we are given proper reason and opportunity to object.

> "Democratic legitimacy demands that where new methods of intelligence gathering and use are to be introduced, they should be on a firm legal basis and rest on parliamentary and public understanding of what is involved, even if the operational details of the sources and methods used must sometimes remain secret."[21]
>
> #Intelligence, DEMOS, Sir David Omand, Jamie Bartlett, Carl Miller

The future

As Local Authorities in the UK seize on the opportunity to use this treasure trove of information about individuals, use of social media by Local Authorities is set to rise and in the future we are likely to see more sophisticated tools used to analyse this data, automate decision-making, generate profiles and assumptions.

---

[17] See: https://privacyinternational.org/examples/2883/woman-jailed-after-posting-pictures-herself-ibiza; https://privacyinternational.org/examples/2884/tender-revealing-israeli-national-insurance-institute-was-trying-access-social-media; https://privacyinternational.org/examples/2882/woman-gets-her-benefits-withdrawn-looking-too-happy-facebook

[18] Privacy International, "Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers", 3 April 2019: https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers

[19] Privacy International, "Bahrain threatens crackdown on followers of anti-government social media accounts", 3 June 2019: https://privacyinternational.org/examples/3069/bahrain-threatens-crackdown-followers-anti-government-social-media-accounts

[20] #Intelligence, Sir David Omand, Jamie Bartlett, Carl Miller

[21] #Intelligence, Sir David Omand, Jamie Bartlett, Carl Miller

FINDINGS

Our investigation has found that:

- A significant number of local authorities are now using 'overt' social media monitoring and this substantially out-paces the use of 'covert' social media monitoring
- If you don't have good privacy settings, your data is fair game for overt social media monitoring.
- There is no quality check on the effectiveness of this form of surveillance on decision making.
- Your social media profile could be used by a Local Authority, without your knowledge or awareness, in a wide variety of their functions, predominantly intelligence gathering and investigations.

"Through our work representing destitute families seeking support and accommodation under section 17 of the Children Act 1989, Matthew Gold & Co regularly encounter local authorities monitoring families' social media accounts as a means to try undermine the credibility of their claims of need.

MG&Co have seen local authorities use information to purport to justify a range of allegations against our clients which prove to be wholly unfounded. When families do not themselves have social media accounts, some local authorities have instead monitored accounts of third parties in their wider family or community context.

As local authorities are often secretive about their practices and sources of information, it can be extremely difficult for our clients to respond to the allegations, many of whom have limited education and speak English as a first language.

Unfortunately, this misuse of information can have extreme consequences for vulnerable children, who by law should be protected. MG&Co has represented multiple families for whom support was been refused or delayed based on misinterpretations of information on their parents or third parties' social media accounts. This has caused hunger, distress, homelessness and the threat of even street homelessness. Yet, upon us challenging the decisions, in every case the local authority provided support because it was accepted that the children were in need".

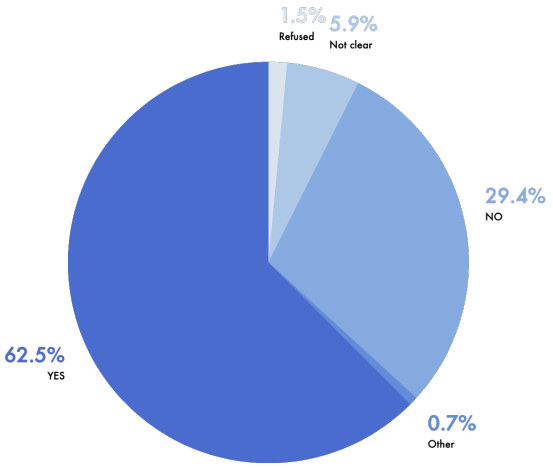
Rachel Etheridge, Matthew Gold Solicitors

ANALYSIS OF FINDINGS

1. A significant number of local authorities are now using 'overt' social media monitoring and this substantially out-paces the use of 'covert' social media monitoring

Overt social media monitoring involves the "Casual (one-off) examination of public posts on social networks as part of investigations undertaken is allowable with no additional RIPA consideration."[22] Whereas "Repetitive examination/monitoring of public posts as part of an investigation" constitutes 'covert' monitoring and "must be subject to assessment and may be classed as Directed Surveillance as defined by RIPA." [23]

Use of overt social media monitoring



	YES	NO	Not clear	Refused	Other
Numbers of LA's	85	40	8	2	1
Percentual (Total = all submissions)	62.5%	29.4%	5.9%	1.5%	0.7%

- We reviewed responses to our FOIA request from 136 Local Authorities
- 62.5% of Local Authorities are using 'overt' social media monitoring
- 31% of Local Authorities are using 'covert' social media monitoring
- 23.1% of Local Authorities who aren't using 'overt' social media monitoring still have a policy/guidance on carrying out this type of surveillance.

[22] Arun District Council Guidance on the Use of Social Media in Investigations
[23] Arun District Council Guidance on the Use of Social Media in Investigations

"The use of the internet as an investigative method is now becoming routine."

London Borough of Ealing RIPA Policy and Guidance

We believe this indicates that 'overt' social media monitoring is a significant tactic used by local authorities. Particularly given that even local authorities who do not use social media monitoring, address it in their policies and guidance. This may signify that this tactic is set to soar in popularity.

Question: Are you able to state how regularly social media is used?

Answer: We estimate to be approximately once or twice a week on average but can vary. Only Facebook is used.

Allerdale Borough Council

As noted in Colchester's 'Use of Social Media in Investigations Policy and Procedure 2018/19'

Social Media has become a significant part of many people's lives. By its very nature, Social Media accumulates a sizable amount of information about a person's life, from daily routines to specific events. Their accessibility on mobile devices can also mean that a person's precise location at a given time may also be recorded whenever they interact with a form of Social Media on their devices. **All of this means that incredibly detailed information can be obtained about a person and their activities.**

Social Media can therefore be a **very useful tool when investigating alleged offences with a view to bringing a prosecution in the courts.** The use of information gathered from the various different forms of Social Media available can go some way to proving or disproving such things as whether a statement made by a defendant, or an allegation made by a complainant, is truthful or not. However, there is a danger that the use of Social Media can be abused, which would have an adverse effect, damaging potential prosecutions and eve leave the Council open to complaints or criminal charges itself.

Of those who are using covert social media monitoring, in response to the question "(c) If the Local Authority has conducted covert social media monitoring, please confirm the number of RIPA warrants obtained in the last two years for this purpose" we received the following updates:

Local Authority	Number of RIPA Warrants obtained in the last two years for covert social media monitoring
Blaenau Gwent County Borough Council	2
Bromley Borough Council	1
Devon County Council	2
Havant Borough Council	1
Isle of Anglesey Council	3
Leicestershire County Council	RIPA warrants: in the period between 1 October 2017 and 1 May 2019, 1 directed surveillance and 5 covert SOCMINT were approved. OVERT SOCMINT: 13 authorisations granted between Sept 2016 - Sept 2019.
North Yorkshire County Council	The following approvals were sought and granted for directed surveillance and use of CHIS in connection with the sale of goods via Facebook. Date Number of approvals 1 October – 30 September 2018/19 1 (counterfeit goods) 1 October – 30 September 2017/18 2 (fireworks)
Oxfordshire County Council	6
Southampton City Council	1
Suffolk County Council	6
Surrey County Council	1
West Dunbartonshire Council	3
West Sussex County Council	8

2. If you don't have good privacy settings, your data is fair game for overt social media monitoring.

Based on guidance from the Investigatory Powers Commissioner[24], Local Authority policies reflect the belief that "the author has a reasonable expectation of privacy if access controls are applied." But "where privacy settings are available but not applied the data may be considered open source and an authorisation [to access it] is not usually required."

We are concerned that the arbitrary distinction of privacy settings to decide whether or not something is 'open source' in relation to social media is flawed and unsophisticated. As noted by authors Lilian Edwards and Lachlan Urquhart, privacy settings constantly change and can apply differently to different content. In

[24] Office of Surveillance Commissioners, Procedures and Guidance, "Oversight arrangements for covert surveillance and property interference conducted by public authorities and to the activities of relevant source", July 2016 : https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf

addition, social media sites are motivated by making user content as public as possible and thus difficult for an individual to protect. We further note they may differ depending on other factors such as jurisdiction and device used.

> …privacy settings vary from platform to platform and also change constantly over time in a way that requires constant vigilance of users to maintain a privacy status quo. Different privacy settings, and different changes, apply to different types of content e.g. posts, comments, groups, photos, friends list etc. On most sites, as with Facebook, the overwhelming motivation is to make as much material as possible public to maximise growth of audience and collection of data for marketing revenue. Hence it is well known that many are deluded in their belief that they have adequately protected their privacy via code controls. Indeed Madejski, Johnson and Bellovin found that in a small study of 65 university students, every one had incorrectly managed some of their Facebook privacy settings, thus displaying some personal data to unwanted eyes.
>
> Lilian Edwards and Lachlan Urquhart, 'Privacy in Public Spaces: What Expectations of Privacy do we have in Social Media Intelligence

Local authorities are following the guidance of the Investigatory Powers Commissioner[25], as exemplified in their codes and guidance documents which set out the approach to 'open source material'. As noted in Barnsley MBC's Local Code of Practice, use of open source material prior to an investigation 'should not normally engage privacy considerations' and individuals should expect to have a 'reduced expectation of privacy' if they post publicly.

> "Investigating officers who use social media and the internet generally as a source of information on suspects or potential

[25] Office of Surveillance Commissioners Procedures and Guidance, July 2016
"298.1 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available**; the author has a reasonable expectation of privacy if access controls are applied** … **Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required**. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind."
"**Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required**. The fact that an individual is not told about "surveillance" does not make it covert."
"If an Officer decides to browse a suspect's blog, website or "open" Facebook page (i.e. where access is not restricted to "friends", subscribers or followers) this will not be regarded as covert."
"However, repeat viewing to browse a suspect's profile on "open sources" sites may constitute directed surveillance. in this case, RIPA authorisation for directed surveillance must be sought. "

suspects must be particularly careful to understand how far they may go before a RIPA authorisation is required. **Whilst the use of open source material prior to an investigation should not normally engage privacy considerations**, if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded, RIPA authorisations may need to be considered."

"There may be a **reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain**, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings."

"Where information about an individual is placed on a publicly accessible database … unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. **Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information."**

Other Local Authorities make it very clear that it is up to the individual to check their privacy settings and to post publicly is done 'at their own risk'. Cheshire West and Cheshire state that:

"Some users will not set any privacy settings at all meaning that the information they post is publicly available. Individuals that operate with no, or limited, privacy settings **do so at their own risk**…

Other users will set their privacy settings to the highest control. These people do not want their content to be in the public domain. Respect should be shown to this content under Article 8 of the HRA, as well as the Data Protection Act 2018.

….Whilst data may be considered 'open sources' where privacy settings have not been engaged and legal authorisation to view the information may not be required, the repeat viewing of 'open source' information may be considered directed surveillance and would be considered unlawful unless RIPA authorisation has been sought."

This puts the onus on individuals to understand and check their privacy settings, and fails to recognise that:

1. Privacy settings vary from platform to platform and also change constantly over time in a way that requires constant vigilance of users to maintain a privacy status quo.
2. People share vastly more personal information about themselves, their friends and their networks than they would if a local authority requested this type of information.
3. Control of what data about you is made public on social media is not simply a matter of easy voluntary choice. For example, in 2018 a Facebook bug changed 14 million people's privacy settings[26].

This approach to social media settings further fails to adapt to what society believes should be counted as public or private, or indeed to our own ideas and presumptions about what we post on social media and who should have access to it and for what purposes.

> Social attitudes towards what is private or public, and therefore what counts as intrusive or not, are blurred and changing. It is unclear whether social media platforms are public spaces, private spaces, or something else altogether.
>
> #Intelligence, Demos

3. There is no quality check on the effectiveness of this form of surveillance on decision making

We asked local authorities if they were able to state how regularly social media monitoring is used and if so to provide figures. We examined the responses of those local authorities who stated that they do use overt social media monitoring.

- We reviewed responses to our FOIA request from 136 Local Authorities
- The majority of the local Authorities who conduct 'overt' social media monitoring, do not monitor i.e. audit this use of 'overt' social media monitoring.
- There is no guidance or requirement from the Investigatory Powers Commissioner for local authorities to track and audit the use of overt social media monitoring.

[26] S. Frenkel, The New York Times, "Facebook Bug Changed Privacy Settings of Up to 14 Million Users", 7 June 2018: https://www.nytimes.com/2018/06/07/technology/facebook-privacy-bug.html

- 60% of Local Authorities who use 'overt' social media monitoring do not provide training for staff

The responses to the question which sought to find out whether local authorities were reviewing the use of overt social media monitoring were confusing, which makes it difficult to draw out any statistics from the replies. There was no clear procedure in the guidance or policy documents disclosed.

The large majority of local authorities who use overt social media monitoring appear to have no processes or procedures in place to audit this surveillance tactic, have no idea how often overt social media monitoring is being used nor are therefore able to assess whether it is being used in a way that is legitimate, necessary, proportionate and effective.

Whilst a few local authorities sought to estimate their usage, others said social media monitoring occurred on a daily basis and some said the information might be logged on the case file but not centrally so were not able to respond.

East Dunbartonshire were able to offer figures and stated that their Corporate Fraud team had undertaken 105 social media inquiries since January 2017 which totalled 21 hours and 40 minutes. Rhondda Cynon Taff Council stated that in 2018-19 they conducted 9 investigations; in 2017-18 they conducted 29 investigations and in 2016-17 they conducted 55 investigations. These were either Human Rights Act, non-RIPA or single viewing of social media site investigations.

This lack of clear information indicates there is a risk that overt social media monitoring is being used by officials on an ad hoc basis without any assessment of whether it is effective. The failure to monitor the 'overt' use of social media monitoring raises questions about how Local Authorities can assess whether 'overt' social media monitoring is effective and improves rather than undermines the quality of decision making.

As noted above, even if it was effective, the absence of public and parliamentary debate over use of overt social media monitoring means a failure to assess the legitimate aim, necessity and proportionality of these activities.

When decision making has serious consequences for an individual, this brings the added risk that comes from unequal access to data, unequal access to justice and the inability to challenge incorrect assumptions that influence or determine human decision making[27].

[27] H. McDonald, The Guardian, "AI system for granting UK visas is biased, rights groups claim", 29 October 2019: https://www.theguardian.com/uk-news/2019/oct/29/ai-system-for-granting-uk-visas-is-biased-rights-groups-claim

> "Officers will view social media from time to time in the course of investigations, but these individual observations are not recorded other than in the prosecution file as part of disclosure procedure."
>
> Ashford Borough Council

This failure to assess and audit the effectiveness of overt social media monitoring in intelligence gathering and investigations by local authorities, means local authorities do not assess how correct they are on deciding integrity of motive of an individual based on their social media output; and means they cannot judge whether they are adept in relation to new forms of online behaviour, norms and languages, which can make analysis and verification difficult.

This may become more pronounced if Local Authorities start using social media analytics tools in their investigations, rather than fraud investigators, for example, doing a manual check on someone's Facebook posts.

> These platforms retain otherwise fleeting and contextually limited content[28].

As acknowledged by Arun District Council in their guidance:

> "In using information obtained from the Internet/social networks, it must be recognised that the 'open source' environment is by nature insecure. Information obtained **cannot be assumed to be fact** and should therefore be subject to separate confirmation. Ideally, additional corroborating evidence should be obtained from a more robust source.
>
> As part of the investigation, consideration must also be given to the circumstances of the case and whether the information is, in fact, demonstrating inappropriate activity. (For example, Facebook postings could suggest that a 'sick' employee is engaging in activity that is inconsistent with their condition – however, **without additional medical advice, or independent examination, this cannot be assumed as being the case**). While such information may be introduced into investigative / disciplinary

[28] Daniel Trottier, European Journal of Cultural Studies 2015, Vol.18(4-5) 530-547

> proceedings as potential evidence, it cannot on its own be deemed to be proof in support of an accusation." [29]

Despite not appearing to conduct social media monitoring, based on their FOIA response, Blackburn with Darwen Borough Council have a Procedural Guide which states that investigating officers "should use a process of monitoring what they do on social media right from the start of an investigation. This will assist them with the process of deciding whether or not they will need to complete a RIPA or non-RIPA form" and complete an internal log where they record:

- Reason/justification for the viewing;
- Assessment of the likelihood of accessing private information about individuals whether they are the target or other individuals;
- Date of viewing;
- Pages viewed;
- Pages saved and where saved to
- Private information gathered i.e. any information about an individual's private and family life.

It is not clear whether there is a process to then audit these logs or simple to decide whether "more investigation is required."

Braintree District Council's guidance also states that "Each viewing of an individual's social network account must be recorded" although there is no indication that this is audited.

> "If an allegation is received, or as part of an investigation into an individual, it is necessary to view their social networking site, officers may access the main page of the individual's profile in order take an initial view as to whether there is any substance to the allegation or matter being investigated.
>
> The viewing of an individual's social network account must be reasonable and proportionate.
>
> **Each viewing of an individual's social network account must be recorded."**
>
> Braintree District Council

Bridgend County Council state they do use overt social media monitoring and that:

[29] Arun District Council Guidance on the Use of Social Media in Investigations

> "Overt surveillance must be authorised by Legal Services and the appropriate Head of Service within the investigatory department."

However, when asked whether they could state how regularly social media monitoring is used, they stated they did not hold this information. It is unclear that authorisation is recorded in any way.

Kingston also require 'management approval' before one-off viewing of social media, but they were unable to state how regularly they use social media monitoring, again indicating that approval may not be logged or reviewed.

It appears that even at those Local Authorities where there is a requirement to log activities or seek approval, there is no follow up which would identify poor practices or deficiencies in how overt social media is conducted and whether 'intelligence' gained is used effectively and properly.

4. Your social media profile could be used by a Local Authority, without your knowledge or awareness, in a wide variety of their functions, predominantly intelligence gathering and investigations.

We found that Local Authorities are using 'overt' social media monitoring in the following areas:

- Recovery of unpaid Council Tax arrears
- Debt recovery
- Regulatory Services/Trading standards e.g. allegation of advertising illegal goods
- Neighbourhood Services
- Licensing
- Corporate Anti-Fraud teams / Revenues and benefits
- Environmental investigations
- Children's social care
- Monitoring protests and demonstrations

Allderdale Borough Council's 4-man debt recovery team use social media for recovery of unpaid Council Tax arrears and states that:

> "...the **debt recovery department** occasionally checks employment details by a number of different sources (which may include social media). This is done overtly and is therefore not subject to RIPA."

Overt in this case involves "officers carry out a quick check on Facebook to see if the debtor has stated their employer on there."

However, they state that in order for this to be done:

> "A Liability Order has been granted against the debtor by West Allerdale Magistrates Court, and that they still have arrears outstanding, and also that they have refused to answer the question on our questionnaire which asks them to notify us where they work, so we can do an attachment of earnings."

Barnet London Borough Council state that:

> "Officers in **Regulatory Services** may do an initial one-off check on social media when considering the validity of an allegation that someone is for example advertising illegal goods, but would not repeatedly search social media as officers are aware of the need to consider a RIPA application for directed surveillance.
>
> Licensing would conduct a "one time only" visit to the relevant social media page with a view to collecting evidence for a specified investigation. They would only use it to assist in an investigation if relevant and do not use it for monitoring purposes."

Cambridge County Council use overt social media monitoring in a number of investigations:

> The Council does make use of overt social media intelligence in the course of some investigations (fraud, environmental investigations such as fly-tipping, enforcement of licensed activities such as tattooing).

Cheshire East Council include children's social care:

> Trading standards; regulatory and environmental health services, communications team, **children's social care**.

Leicestershire County Council also focus on children's services:

> Social media monitoring is also being considered for the Safeguarding area within Children's services. However, this is in the

> early stages of development and, as yet, we don't have any firm dates for implementation.

Cheshire West informed us that they are likely to expand use of overt social media monitoring:

> While access to individual's SNS by Council Officers has largely been confined to those undertaking official investigations, for example Trading Standards Officers or members of the Fraud and Investigations team, those activities would be closely supervised, there is growing awareness that a number of other roles, most notably **those relating to care of children and vulnerable adults and Council Tax/Benefits**, may also view SNS as a legitimate information resources.

Kingston discuss use by their community housing team:

> The council's Anti-Fraud Team uses social media intelligence for conducting investigations…The council's **Community Housing Team** use it for investigations that could include reference to public domain data.

Oldham Council use social media monitoring in relation to protests and demonstrations and to identify a groups' activities:

> The Council monitors social media to gather intelligence about community tensions. This would include for example, **finding out about a group's plans to hold protests or demonstrations.** All material accessed is open source. Identification of groups' activities would only be identified because they are publicly stating what they plan to do.

Swindon Borough Council, Internal Audit Services: Use of Social Media for Investigations policy identifies use in relation to homelessness applicants:

> "Officers in Housing, Homelessness and Children's Services informed the Auditor that they or their staff use social media to gather information on clients. **For example, homelessness applicant's Facebook profiles** (open source) **may be viewed to confirm whether information provided by them is true** e.g. where they previously lived. In Children's Services, Social Workers may view the Facebook profiles of parents to establish whether they have broken any agreements between them and the Council e.g. for two parents not to have contact with one another.
>
> …The Council doesn't have a policy that covers the use of social media to gather or verify service users' information, to ensure that an assessment of proportionality with regard to their right to privacy is carried out.

The various use cases outlined above should be seen as part of a broader apparatus being deployed, where social media monitoring plays a role. Privacy International's work 'When Big Brother Pays Your Benefits[30]' examines the use of technology as a magic cure-all to socio-economic and political issues.

Newly established or reformed social protection programmes have gradually become founded and reliant on the collection and processing of vast amounts of personal data and increasingly the models for decision-making include data exploitation and components of automated decision-making and profiling.

Whilst social media monitoring by local authorities in Great Britain, at present, involves a manual check of individuals social media such as their Facebook page, as the use of such monitoring increases and is used in a wide variety of areas in which local authorities are active, so too will the prospect of automating such checks and monitoring. In turn, such practices lead invariably to automated decision-making, profiling and the inherent risks of such practices. This will be at the cost of individuals privacy, dignity and autonomy.

Therefore, is it vital that the collection and processing of personal data obtained from social media as part of local authority investigations and intelligence gathering, are strictly necessary and proportionate to make a fair assessment of an individual. There neds to be effective oversight of use of social media monitoring both overt and covert to ensure that particular groups of people are not disproportionately affected, and where violations of guidance and policies do occur, they are effectively investigated and sanctioned.

We further note that for example Oldham Council uses social media monitoring in relation to protests and demonstrations and to identify a groups' activities. The

[30] Privacy International, When Big Brother Pays Your Benefits: https://privacyinternational.org/taxonomy/term/675

unregulated use of social media monitoring negatively affects the right of freedom of peaceful assembly. It has a chilling effect on individuals wishing to organise online, as well as using social media platforms to organise and promote peaceful assemblies[31].

[31] Privacy International, Submission on Article 21 of the International Covenant on Civil and Political Rights , February 2019: https://privacyinternational.org/sites/default/files/2019-03/Submission%20on%20Article%2021%20of%20ICCPR_0.pdf

RECOMMENDATIONS

To the Investigatory Powers Commissioner:

- Call for guidance setting out guidelines, with concrete examples, by 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 just and proportionate to these legitimate aims;
    - Whether repeated or persistent viewing constitutes directed surveillance.

To the local authorities:

- Local authorities should refrain from using social media monitoring, and should avoid it entirely where they do not have a clear, publicly accessible policy regulating this activity.

Where exceptionally used:

- Local authorities should use social media monitoring only if and when in compliance with their legal obligations, including data protection and human rights.
- Every time a local authority employee views a social media platform, this is recorded in an internal log including, but not limited to, the following information:
    - Date/time of viewing, including duration of viewing of a single page
    - Reason/justification for viewing and/or relevance to internal investigation
    - Information obtained from social platform
    - Why it was considered that the viewing was necessary
    - Pages saved and where saved to
- Local authorities should develop internal policies creating audit mechanisms, including:
    - The availability of a designated staff member to address queries regarding the prospective use of social media monitoring, as well as her/his contact details;
    - A designated officer to review the internal log at regular intervals, with the power to issue internal recommendations

History of the regulators' concerns

The Office of Surveillance Commissioners (OSC) and subsequently the Investigatory Powers Commissioner (IPC) regulate and oversee how public authorities use the investigatory powers available to them under existing law.

Below are extracts from the annual reports of the OSC and IPC which relate to Local Authorities use of social media monitoring.

The Chief Surveillance Commissioner, The Rt Hon Sir Christopher Rose's Annual Report 2011 - 12[32] did not refer to social networks but to overt investigations using the internet as a surveillance tool, stating that:

> "5.17 A frequent response to my Inspectors' enquiries regarding a reduction in directed surveillance is **that 'overt' investigations using the Internet suffice.** My Commissioners have expressed concern that **some research using the Internet may meet the criteria of directed surveillance**. This is particularly true if a profile is built by processing data about a specific individual or group of individuals without their knowledge.
>
> 5.18 **There is a fine line between general observation, systematic observation and research** and it is unwise to rely on a perception of a person's reasonable expectation or their ability to control their personal data. Like ANPR and CCTV, the Internet is a useful investigative tool but they each operate in domains which are public and private. As with ANPR and CCTV, it is inappropriate to define surveillance solely by the device used; the act of surveillance is of primary consideration and this is defined at section 48(2-4) of RIPA (monitoring, observing, listening and recording by or with the assistance of a surveillance device). **The Internet is a surveillance device as defined by RIPA section 48(1). Surveillance is covert "if, and only if, it is conducted in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is, or may be taking place." Knowing that something is capable of happening is not the same as an awareness that it is or may be taking place.** The ease with which an activity meets the legislative threshold demands improved supervision."

The Chief Surveillance Commissioner, The Rt Hon Sir Christopher Rose's Annual Report first referred to social network sites in 2012-13[33] stating that:

---

[32] Office of Surveillance Commissioners, Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2011-2012: https://www.ipco.org.uk/docs/osc/OSC%20Annual%20Report%202011-12.pdf

[33] Office of Surveillance Commissioners, Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2012-2013: https://www.ipco.org.uk/docs/osc/OSC%20Annual%20Report%202012-13.pdf

> "2.4 All public authorities have struggled with the **use of the Internet for investigations, particularly social network sites**. A particular difficulty is the desire of national bodies to apply a doctrinaire approach which invites **error if facts specific to each case are ignored or poorly considered**."
>
> "5.7. I am encouraged by the increasingly mature debate relating to the use of the Internet for investigative purposes, especially the use of social networking sites. It is not always adequate to conflate the off-line with the on-line worlds and I am satisfied that some investigations require authorisation. There are points of detail to work out, particularly in relation to repeated viewing of a publicly available site but, in the main, RIPA Part II can be used effectively. I will continue to support the production of accurate Home Office and ACPO guidance. But it is important to bear in mind that it is not always possible to give definitive answer as to whether particular activity requires authorisation: facts are infinitely variable. Where there is doubt authorisation is prudent."

The Chief Surveillance Commissioner, The Rt Hon Sir Christopher Rose's Annual Report 2013-14[34] referred to social network sites in stating that:

> "5.30 This is now a deeply embedded means of communication between people and **one that public authorities can exploit for investigative purposes**. I am reasonably satisfied that there is now a heightened awareness of the use of the tactic and the advisable authorisations under RIPA that should be considered. **Although there remains a significant debate as to how anything made publicly available in this medium can be considered private**, my Commissioners remain of the view that **the repeat viewing of individual "open source" sites** for the purpose of intelligence gathering and data collation should be considered within the context of the protection that RIPA affords to such activity.
>
> 5.31 In cash-strapped public authorities, it might be tempting to **conduct online investigations from a desktop**, as this saves time and money, and often **provides far more detail about someone's personal lifestyle, employment, associates etc**. But just because one can, do not mean one should. The same considerations of privacy and especially collateral intrusion against innocent parties, must be applied regardless of the technological advances. It is worth repeating something I said in my 2011-2012 report, paragraph 5.18...[see above].

[34] Office of Surveillance Commissioners, Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2013-2014: https://www.ipco.org.uk/docs/OSC%20Annual%20Report%202013-14.pdf.pdf

> 5.32 Access to social networking sites by investigators in all public authorities is something we examine on inspections. Many, particularly the law enforcement agencies, now have national and local guidance available for their officers and staff. **However, many local authorities and government departments have still to recognise the potential for inadvertent or inappropriate use of the sites in their investigative and enforcement role**. Whilst many have warned their staff of the dangers of using social media from the perspective of personal security and to avoid any corporate damage, **the potential need for a RIPA authorisation has not been so readily explained**.
>
> 5.33 I strongly advise all public authorities empowered to use RIPA **to have in place a corporate policy on the use of social media in investigations.** Some public authorities have also found it sensible to **run an awareness campaign**, with an **amnesty period for declarations of any unauthorised activity or where, for example, officers have created false personae to disguise their online activities**.

The Chief Surveillance Commissioner, The Rt Hon Sir Christopher Rose's Annual Report 2014-15[35] stated that:

> Social Networks
>
> 5.42. **Perhaps more than ever, public authorities now make use of the wide availability of details about individuals, groups or locations that are provided on social networking sites and a myriad of other means of open communication between people using the Internet and their mobile communication devices**. I repeat my view that **just because this material is out in the open, does not render it fair game**. The Surveillance Commissioners have provided guidance that certain activities will require authorisation under RIPA or RIP(S)A and this includes repetitive viewing of what are deemed to be "open source" sites for the purpose of intelligence gathering and data collation.
>
> 5.43. I am pleased to see that law enforcement agencies have provided and are continually developing detailed guidance to their officers and members of staff about accessing such sites, and the College of Policing is working closely with national leads and other interested parties to ensure a consistent and lawful approach.
>
> 5.44. **Many local authorities have not kept pace with these developments. My inspections have continued to find instances**

[35] Office of Surveillance Commissioners, Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2014-2015: https://www.ipco.org.uk/docs/OSC%20Annual%20Report%202014-15.pdf

> **where social networking sites have been accessed, albeit with the right intentions for an investigative approach, without any corporate direction, oversight or regulation**. This is a matter that every Senior Responsible Officer should ensure is addressed, lest activity is being undertaken that ought to be authorised, to ensure that the right to privacy and **matters of collateral intrusion have been adequately considered** and staff are not placed at risk by their actions **and to ensure that ensuing prosecutions are based upon admissible evidence**.

In the Annual Report of the Chief Surveillance Commissioner, The Rt Hon Lord Judge 2015-2016[36] he gave the following examples in relation to social networks:

> "Example 1: In one particular public authority, once a task is allocated to an internet desk officer, that officer undertakes research using a non attributable computer which stands alone from the authority's main network. Although it is said that the staff do not use false personas, the activity they undertake is calculated to be covert so as to minimise the risk of compromise to ongoing investigations. Staff typically undertake research on one occasion, although this singular research activity may extend over several hours and involve research of different social media sites linked to the subject. There is a perception by staff within the unit that investigators are reluctant to, or dissuaded from, making more than one request for research to be undertaken on the same subject. The head of the unit believes that investigators are missing opportunities for securing valuable intelligence by restricting their request to singular research; this is a view shared by the inspection team. **Very rarely are any requests for research of open source material or social media supported by an authorisation for directed surveillance**. In a twelve month period the unit has processed 3,561 requests for internet research, on just two occasions directed surveillance authorisations supported the activity being undertaken.
>
> Example 2: In another public authority, one matter absent from the various policy and guidance documents is the **use of the internet for investigative purposes. This technique of investigation and research is expanding exponentially with all manner of new technology and although some knowledge and awareness was evident during discussion with staff, further guidance and advice would benefit investigators and Authorising Officers alike. The key consideration when viewing publicly available information where no privacy settings have been applied, often referred to as 'open source' material, is the repeated or**

[36] Office of Surveillance Commissioners, Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2015-2016: https://www.ipco.org.uk/docs/OSC%20Annual%20Report%202015-16.pdf

systematic collection of private information. Initial research of social media to establish a fact or corroborate an intelligence picture is unlikely to require an authorisation for directed surveillance; whereas **repeated visits** building up a profile of a person's lifestyle would do so. Each case must be considered on its individual circumstances and early discussion between the investigator and the Authorising Officer is advised to determine whether activity should be conducted with or without the protection of an authorisation."

The Annual Report of the Chief Surveillance Commissioner, The Rt Hon Lord Judge 2016-2017[37] stated:

"4.3 From time to time my Inspectorate is asked why, given that no authorisation has been granted by an individual authority since the previous inspection some three years earlier, the process of inspection and oversight is necessary. The short answer is unequivocal. While local authorities remain vested with the power to deploy covert surveillance, regardless of actual use, the appropriate structures and training must remain in place so that if and when the powers do come to be exercised, as they may have to be in an unexpected and possibly emergency situation, the exercise will be lawful. So, for that reason alone the process of inspection must continue. There is a further consideration. The inspection may reveal inadvertent use and misuse of the legislative powers. **The steady expansion in the use of the social media and Internet for the purposes of investigative work provides a striking example of a potential new problem which came to light through the inspection system. Local authority officials, vested with burdensome responsibilities for, among others, the care of children and vulnerable adults, are, like everyone else, permitted to look at whatever material an individual may have chosen to put in the public domain. This is entirely lawful, and requires no authorisation. However, repeated visits to individual sites may develop into an activity which, if it is to continue lawfully, would require appropriate authorisations. Local authorities must therefore put in place arrangements for training officials into a high level of awareness of these risks. Without the inspection process this problem might never have been identified.**

15.2 As discussed earlier one major consequence of the OSC inspections has been the emergence, during the course of discussions, of investigations being made by public authorities through use of social media and the Internet. **For example, it may help to show whether counterfeit good are being offered for sale**

[37] Office of Surveillance Commissioners, Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2016-2017: https://www.ipco.org.uk/docs/OSC%20Annual%20Report%202016-17.pdf

on a Facebook page, or reveal that someone who claims to be living alone as a single parent has a social media page which provides a different story, or perhaps, particularly sensitive, enable a check to be made whether concerns about the welfare of a child or vulnerable adult may be justified. When individuals choose to go public or advertise themselves, they cannot normally complaint that those who look at their social media sites are disregarding their rights to privacy. However if the study of an individual site becomes persistent, issues under the legislation may arise.

15.3 The resources available to the OSC do not enable me to say positively that issues relating to the use of social media sites have arisen or are arising in every local authority. What matters is that this potential certainly exists. Senior officials at local authorities should therefore be made aware of it and have the necessary policy documents and training and awareness arrangements in place to address it. This issue has been recognised in the forthcoming Home Office and Scottish Government Codes of Practice (which will be issued at a convenient date after the introduction of the Investigatory Powers Act 2016). However, in advance of the issue, and because of repeated findings in reports made to me by Inspectors and Assistant Surveillance Commissioners throughout this year, I acted on my own initiative. I therefore wrote to all local authorities in April 2017 explaining my concerns, and urging them to undertake internal checks of the use of social media by no doubt well-intentioned members of their staff, and to ensure that appropriate guidance and training should be provided.

15.4 An extract from the letter reads:

"it has become steadily more apparent that a number of officers working for public authorities, particularly those with responsibilities for the care of children and vulnerable adults have started to use the [social media and internet] sites, acting in good faith and on their own initiative. RIPA issues do not normally arise at the start of any investigation which involves accessing "open source" material, but what may begin as lawful overt investigation can drift into covert surveillance which falls within the legislation. Although the investigation of crime is not normally a "core function" of the Council, the protection of children and vulnerable adults certainly is, and any continuing and deeper study of the social media site in question would only be justified by the exercise of that protective function.

These are complex legislative provisions, and without appropriate training and awareness council officers cannot be expected to appreciate and apply them. They may therefore act unlawfully. Ignorance would provide no defence to them personally, nor to the Council for which they were working.

> The Surveillance Commissioners have issued further guidance on this issue, and identified circumstances when an appropriate authorisations under the legislation would be required or advisable. The guidance is available on the OSC website as a public document, with the OSC Procedures Guidance. Note 289 is relevant and I highlight it for your attention.
>
> It would be sensible for an internal audit of the use of social media sites and Internet for investigative or official business made across all departments be undertaken now. That would provide the necessary information about the extent to which formal training or awareness of these complex provisions is required."
>
> 15.5 A copy of this letter was sent to the Chair of the Local Government Association and the national police lead for child protection issues, Chief Constable Simon Bailey of the Norfolk Constabulary.
>
> 15.6 As I reported last year, many local authorities have first-class arrangements in place for the use of covert tactics, even if, as a matter of policy, they do not intend to deploy them: others do not. Where necessary arrangements to ensure compliance are not in place, I require a report from the Chief Executive after a given period, say six months, about how the inadequacies have been addressed, and indicating that a further inspection may have to be arranged. There have been, and will continue to be occasional inspection revisits. One such revisit will have taken place by the time this report is published. I should, however, highlight that the problem of the non-compliant local authority should be kept in perspective. These authorities very rarely use or attempt to use statutory powers, and the occasions when they have been in breach of the legislative provisions remain very rare indeed. The point, as one of my Inspectors helpfully paraphrased it, is that while they are vested with these significant powers they should remain "match fit". The inspection process provides both an encouragement and a check that they are.

The Investigatory Powers Commissioner replaced the Surveillance Commissioner. The Investigatory Powers Commissioner, Sir Adrian Fulford's Annual Report 2017-2018 states:

> 4.37 Local authority guidance on surveillance does not always address how investigators should use social media or where they may need an authorisation. The 2018 revised Home Office code of practice for surveillance contains helpful advice local authorities can incorporate into their policy documents and training.

4.38 Our inspectors were particularly impressed by Durham Country Council, whose senior responsible officer commissioned a helpful audit across the organisation on the 'Use of social media in Covert Investigations', to evaluate and report their system is adequate and appropriate for this purpose. We commend this approach.

Home Office Covert Surveillance and Property Interference Code of Practice, August 2018[38]

Below are relevant extracts from the Home Office Covert Surveillance and Property Interference Code of Practice, August 2018, which relate to social media monitoring conducted by Local Authorities.

This document has informed the policies and guidance documents produced by Local Authorities in relation to social media monitoring. A number policies and guidance documents have been disclosed to Privacy International in response to Freedom of Information Act requests.

> Online covert activity
>
> 3.10 **The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve.** It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. **Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations**. But if the study of an individual's online presence becomes persistent, or **where material obtained from any check is to be extracted and recorded and may engage privacy considerations**, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.
>
> 3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).
>
> 3.12 **In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place.** Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the

[38] Home Office, Covert Surveillance and Property Interference Revised Code of Practice, August 2018: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

activity. Conversely, **where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt** and a directed surveillance authorisation will not normally be available.

3.13 As set out in paragraph 3.14 below, depending on the nature of the online platform, **there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain**, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

3.14 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. **Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.**

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. **Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered.** These considerations apply regardless of when the information was shared online. See also paragraph 3.6.

Example 1: A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.

Example 2: A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)

Example 3: A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

3.16 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

3.17 Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.32).

Example: Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad

thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

ANNEX A: FOIA

Dear Sir/Madam,

Freedom of information act request

RE: Social media monitoring / social media intelligence

FOIA REQUEST

For definition of social media intelligence please see background explanation below. We further note the comments of the Office of Surveillance Commissioners Annual Report 2016 cited below.

1. In 2016 the Rt Hon Lord Judge, then Chief Surveillance Commissioner, wrote to all Local Authorities regarding use of social media in investigations. Please confirm whether you are aware you received this letter and:
(a) Provide a copy of your response; (please confirm if you did not respond)

(b) Provide a copy of any internal audit relating to social media use arising out of Rt Hon Lord Judge's recommendations; (please confirm if you did not conduct an internal audit and state whether any internal audit of social media use has taken place since 2016).

(c) Provide a copy of your corporate policy on the use of social media in investigations. (please confirm if you do not have one)

(d) Please confirm whether a follow up audit was conducted by the Surveillance Commissioner's Office which was exclusively or partially related to social media use in investigations by your Local Authority.

2. Does your Local Authority conduct overt and/or covert social media intelligence in some or all of its work?

(a) If yes, please specify whether this includes profiling individuals, conducting investigations, monitoring individuals, monitoring groups, monitoring locations, gathering intelligence, for recruitment purposes.

(b) If your Local Authority does conduct social media intelligence/monitoring, please specify whether this includes both or either overt or covert monitoring of social media.

(c) If the Local Authority has conducted covert social media monitoring, please confirm the number of RIPA warrants obtained in the last two years for this purpose.

3. If the Local Authority conducts social media intelligence, please provide a copy of any current guidance/policies/internal guidance/code of practice or any other such written material used by/available to the local authority or those

working on behalf of the local authority to conduct SOCMINT, the monitoring or accessing of information published on social media that is either publicly available or requires additional access e.g. to be friends with an individual, to have password and login details.

4. If you conduct overt or covert social media intelligence relating to social media platforms, please provide a copy of:
(a) Relevant [sections of the] privacy policy;
(b) the data protection impact assessment;
(c) privacy impact assessment;
(d) equality and human rights impact assessment
(e) training materials for those conducting social media intelligence.

Please state if you do not have any of the above.

5. Please provide a copy of any other template/form/document currently used (or to be used with the next three months) by the local authority or fraud investigator (or team) in the conduct of social media monitoring

6. Please confirm whether or not your local authority has purchased or uses software and/or hardware to conduct social network / social media monitoring and/or in relation to sentiment analysis.

(a) If yes, please state the name of the company / provider.

(b) If no, please state whether the local authority has developed internal methods to conduct social media / social network monitoring.

7. Please confirm, if not stated in the guidance (question 3), the policy on deletion of data obtained from social networking sites.

8. If no documents (question 3) exist, or if the following is not covered in the documents which do exist, please explain:
a. In what areas of the local authority's work is social media monitoring used
b. What criteria must be satisfied in order for social media monitoring to be carried out
c. Who must authorise the request to conduct social media monitoring
d. What is the process for conducting social media monitoring
e. How long is data collected and retained?
f. Is there any process for requesting deletion?

9. Are you able to state how regularly social media monitoring is used? If so, please provide the figures.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321

privacyinternational.org