Message for Designated Officers

Dear all,

As you will be aware, your services are required to record covert surveillance activity carried out using social media, which will be submitted in response to quarterly requests from the SRO (Elin Prysor) or SRO Representative (Harry Dimmack). I am writing to request your activity reports of covert surveillance carried out on social media and details of any covert online personas held by your services for the period of the [DATE] to the [DATE].

Further details on the activity which requires reporting are set out below.

It is important that staff are aware that any systematic, repeated viewing of an individual's online presence, covertly, and which may engage privacy considerations, requires the consideration of a RIPA authorisation. Examples of covert surveillance could include an Officer accessing a private Facebook post/individual page of a member of the public and that person is unaware the Officer is doing this (perhaps, for example, the Officer is using a personal Facebook account that does not state who the Officer is, their role in the Council or why they are accessing the page).

Your services are required to:

1. Record information/data relating to covert social media/on-line surveillance, including on-line personas (* see below)
2. Identify a Designated Officer
3. Provide this data to the Designated Officer; and
4. The Designated Officer must provide the information to the SRO (Elin Prysor) or the SRO's Representative (Harry Dimmack) every 4 months.

As a Designated Officer, you are required to maintain a record of the following information:

- Which media site(s)/on-line profile(s) have been visited;
- Was access to the media site(s)/on-line profile(s) restricted (provide details);
- When were the media site(s)/on-line profile(s) visited;
- by whom (Officer/User);
- on whose request;
- who authorised;
- Details of the surveillance- e.g. case reference, operation, investigation
- date of request;
- date of access;
- on which profile/social media account;
- was an on-line persona/false profile/false identity used? If so, which?;
- Provide details of on-line persona/false profile/false identity address/contact details/pseudonyms;
- was an official corporate profile used? If so, which;
- how many viewings
- length of viewing(s);
- for what purpose/rationale was the media site(s)/on-line profile(s) visited;
- Confirmation that the person whose identity is used has explicitly consented in writing, and their protection considered, and details of what is/is no to be done;
- Aim/information desired;
- was the subject aware;
- what data was obtained (including collateral information);

- what was done with any resultant product;
- Details of Social Media relevant to Application;
- Explanation why on-line persona required and alternative methods considered;
- Confirmation as to whether a Risk Assessment has been considered/carried out; and
- Any result, including any risk to Officer (and if not, why not).

You may use the attached spreadsheet to record this information and submit as requested on a quarterly basis.

A register of the data will be compiled and retained by the SRO, and disclosed to the IPCO inspector upon request/at time of inspection.

In response to suggestions made during the Council's recent IPCO Inspection, returns will be subject to quality control, further enquiries and a dip sampling exercise in order to assess their accuracy.

We are grateful for your co-operation in providing this information.

Regards,