ASSOCIATION OF CHIEF POLICE OFFICERS

Online Research and Investigation

Examples Supplement

This document is intended to provide guidance to police officers or staff engaged in research and investigation across the internet.

This guidance is not a source of law but is subject to the legislation and to the statutory Codes of Practice.

It is being circulated in the interests of promoting good practice and consistency across law enforcement.

If you would like any advice regarding the examples provided in this document please contact the ACPO preferred source of advice at the NCA Specialist Operations Centre on 0845 000 5463

Introduction

The examples given in this document are supplementary to the ACPO guidance on Online Research and Investigation.

As stated in that guidance, whenever you are using the internet to gather intelligence or evidence you must consider whether you are likely to interfere with a person's Article 8 right to respect for their private and family life and, if so, whether you should seek authorisation under RIPA for your conduct. The principles in this guidance have been prepared to help you identify whether such authorisation may be appropriate. It is also essential to consider the effect of any collateral intrusion on the private and family life of other people not directly connected with the subject of the research or investigation.

There can be no "one size fits all" solution when making this consideration and it is important to stress that case by case judgement is vital**.** However the examples given on the following pages may assist the decision making process of those who are conducting the activity.

If you are unsure whether it would be appropriate to seek authorisation in any particular circumstances further advice can be obtained from the ACPO preferred source of advice at the NCA Specialist Operations Centre on 0845 000 5463 who will provide advice on the specific facts of your own case based on the reasoning behind the guidance.

Example 1

Police researchers using a police profile on an attributable device to view, for a specific policing purpose, a website with no access restrictions or an open profile on a social networking site.

The activity under consideration involves the simple viewing of open source information, not subject to any privacy settings and without any subterfuge on the part of the police. It is unlikely that this activity, whether on a one off or repeated basis and irrespective of whether it is in regard to a specific operation about a known individual, will interfere with any person's Article 8 rights and RIPA authorisation need not be sought.

Example 2

HMRC researchers using an HMRC profile to view, for a specific policing purpose, a number of open profiles on a social networking site. They will "download screen capture" anything of evidential value.

The activity under consideration involves the viewing and recording of open source information, not subject to any privacy settings and without any subterfuge on the part of the police. The viewing of the material is unlikely, whether on a one off or repeated basis and irrespective of whether it is in regard to a specific operation about a known individual, to interfere with any person's Article 8 rights and RIPA authorisation need not be sought. However, the retention and processing of the information may result in an Article 8 interference. Compliance with the principles of the Data Protection Act should render any such interference lawful.

Example 3

NCA researchers using a false persona profile to view, for a specific policing purpose, a number of open profiles on a social networking site. There will be no interaction with these profile owners or other users of the social networking site.

The activity under consideration involves the simple viewing of open source information, not subject to any privacy settings. The viewing of the material, whether on a one off or repeated basis and irrespective of whether it is in regard to a specific operation about a known individual, is unlikely to interfere with any person's Article 8 rights and RIPA authorisation need not be sought. Whilst the creation and use of a false persona is likely to be a breach of the social networking site's terms and conditions it is not, in itself, unlawful. The legal position as to whether the use of a false persona would make any access to data "unauthorised" under the terms of the Computer Misuse Act is unclear but the risk of criminal liability arising is considered extremely remote.

Example 4

Police researchers using a false persona profile to view, for a specific policing purpose, a number of open profiles on a social networking site. There will be no interaction with these profile owners or other users of the social networking site but they will "download screen capture" information of evidential and intelligence value.

The activity under consideration involves the viewing and recording of open source information, not subject to any privacy settings. The viewing of the material, whether on a one off or repeated basis and irrespective of whether it is in regard to a specific operation about a known individual, is unlikely to interfere with any person's Article 8 rights and RIPA authorisation need not be sought. Whilst the creation and use of a false persona is likely to be a breach of the social networking site's terms and conditions it is not, in itself, unlawful. The legal position as to whether the use of a false persona would make any access to data "unauthorised" under the terms of the Computer Misuse Act is unclear but the risk of criminal liability arising is considered extremely remote. The retention and processing of the evidential/intelligence information may result in an Article 8 interference. Compliance with the principles of the Data Protection Act should render any such interference lawful.

Example 5

HMRC researchers using a false persona profile to view, for a specific policing purpose, a profile on a social networking site. The privacy settings of the profile have been activated in order to allow access only to the profile owner's "friends". The researcher will send a "friends request" which if accepted will allow viewing of but there will be no interaction beyond the sending and acceptance of the friends request. They will "download screen capture" information of evidential and intelligence value.

The activity under consideration involves the viewing and recording of restricted access information. The viewing and recording of this material is, because it is not of an entirely public nature, considered likely to interfere with a person's Article 8 rights. As there is no intention to interact the sending and acceptance of the friend request is unlikely to constitute a "relationship" and authorisation as a CHIS is not considered appropriate. Although CHIS authorisation is not appropriate it is considered good practice that friends requests are only sent by staff trained to undertake undercover online activity. This activity is considered to be covert surveillance which is likely to obtain private information about a person and RIPA authorisation for directed surveillance should be sought. The retention and processing of the evidential/intelligence information should be done in accordance with the principles of the Data Protection Act.

Example 6

NCA researchers using a false persona profile to view, for a specific policing purpose, a profile on a social networking site. The privacy settings of the profile have been activated in order to allow access only to the profile owner's "friends". The researcher will send "friends requests" and if accepted they will interact with the profile owners using their false persona. They will "download screen capture" information of evidential and intelligence value.

The activity under consideration involves the viewing and recording of restricted access information. The viewing and recording of this material is, because it is not of an entirely public nature, considered likely to interfere with a person's Article 8 rights. The interaction between the researcher and the profile owner is considered to be a relationship which, as it is in a false persona, is a relationship maintained for a covert purpose. Authorisation as a CHIS should therefore be sought. This activity should only be done by staff trained to undertake undercover online activity. The retention and processing of the evidential/intelligence information should be done in accordance with the principles of the Data Protection Act.