

Freedom of Information Act 2000 (Section 50)

Decision Notice

Date 13 February 2007

Public Authority: London Borough of Camden
Address: Camden Town Hall
Judd Street
London
WC1H 9JE

Summary

The complainant asked Camden Council to provide him with the identities of all residents who had been made the subject of Anti-Social Behaviour Orders (ASBOs).

The Council provided the complainant with an edited version of its ASBO database. Information that could identify individuals was withheld by the Council under sections 31 and 40 of the Act. The Commissioner is not satisfied that section 31 was engaged. He decided that the Council was wrong to rely upon section 40 to redact the names of all the individual recipients of ASBOs but that redaction could be justified in some cases.

The Commissioner requires the public authority to provide the complainant with a full version of its ASBO database but after redaction of names in those cases where:

- reporting restrictions were imposed by the court at the original ASBO hearing or at any hearing for breach;
- the ASBO did not proceed beyond interim status;
- the public authority is satisfied that the ASBO recipient is particularly vulnerable and would be put at real risk by disclosure; or
- the ASBO has now expired.

The Commissioner's Role

1. The Commissioner's duty is to decide whether a request for information made to a public authority has been dealt with in accordance with the requirements of Part 1 of the Freedom of Information Act 2000 ('the Act'). This Notice sets out his decision.

The Request

2. On 11 May 2006 the complainant requested the following information from the Council:

'We understand that Camden possesses an electronic database of all the ASBOs issued in the borough, both current and expired and that this contains basic information of names, addresses, terms of the orders and nature of the order. We request a copy of this database to be supplied to us by email in electronic form. All the information in it of course, is in the public domain, because these orders are made in public and indeed, are supposed to be publicly known about. They can be specifically publicised by councils if they wish.'
3. On 26 May 2006 the Council advised the complainant that its electronic ASBO data base did not include details of individuals' addresses. The Council provided the complainant with an edited version of the data base with names of individuals redacted under section 40 (personal information) and section 31 (law enforcement) of the Act.
- 4, On 1 June 2006 the complainant requested an internal review of the Council's decision and on 20 June 2006 the local authority upheld its original decision to withhold the redacted information.

The Investigation

Scope and Chronology of the case

5. The complainant contacted the Commissioner on 20 June 2006 to formally complain about the Council's refusal to provide the identities of residents who had been issued with Anti-Social Behaviour Orders.
6. The complainant argued that:
 - (a) Names of individuals who are subject to Anti Social Behaviour Orders are already in the public domain. As ASBOs are public orders of the court, the recipients of such orders have an expectation of publicity.
 - (b) The Council gives insufficient weight to the public interest in justice taking place in public.
 - (c) The Council selectively publish names of individuals who are subject to ASBOs and it therefore has no rational basis for refusing to disclose the other names.
 - (d) Whilst there may be an argument for redacting names of juveniles when orders restrict publicity, this is a limited issue and should be considered separately.

- (e) The Council fails to show how the release of individuals' names (other than those of juveniles) would prejudice law enforcement.
7. The Commissioner requested a copy of the ASBO database from the Council. He asked the Council to clarify why addresses of individuals were not included and was informed that because the Metropolitan Police held the substantive information on individuals that were subject to ASBOs, the Council felt duplication of addresses to be unnecessary.
 8. The complainant had informed the Commissioner that he required the names of individuals in order to ascertain how often residents had been issued with repeat orders (and in this way gauge the effectiveness of ASBOs). The Commissioner considered whether informal resolution of the complaint might be achieved by modification of the data to conceal identities. He asked the Council if it would substitute identifiers in place of names and asked the complainant whether this would serve his requirements. The Council stated that it was willing to provide the substitution, however, the complainant still considered the disclosure of names to be necessary.

Background Information

9. Anti-social behaviour orders ("ASBOs") are civil court orders which protect the community from behaviour that has caused, or is likely to cause, harassment, alarm or distress. They are preventative orders, designed to curb repetition of anti-social behaviour by imposing restrictions on behaviour. ASBOs were introduced by Section 1 of the Crime and Disorder Act 1998 and first used in 1999. As modified by the Police Reform Act 2002 and the Anti-Social Behaviour Act 2003, orders can ban individuals from entering certain areas or carrying out specific acts. They run for a minimum period of two years. Over two hundred ASBOs were issued to individuals in the Camden area during the period relating to the complainant's request for information. The majority of these orders were made against adults for drug related offences.

Analysis

Exemptions

Section 40 (personal information)

10. The Council relied upon section 40 of the Act to withhold the requested information. It stated that the information constituted data within the definition of section 1(1) of the Data Protection Act 1998 (DPA) and in its view disclosure would contravene the first and second data protection principles.
11. The Council maintained that:
 - the information was held specifically for ASBO monitoring and enforcement. Although enforcement may require the publicising of certain personal information,

this must be local, reasonable and proportionate. The Council contended that disclosure would go beyond this. In its view, individuals subject to ASBOs would not expect the information to be disclosed outside their locality

- several cases recorded on the database were only at the interim stage of proceedings where no finding of fact was required
- a number of individuals who had been issued with ASBOs were under the age of eighteen and were therefore considered to be vulnerable
- some individuals were subject to publicity restrictions by the court.

12. The Commissioner is satisfied that the requested information (i.e. that redacted by the Council) is personal data as defined in the DPA. The DPA defines personal data as:

*... data which relate to a living individual who can be identified –
a) from those data, or
b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller...*

13. The complainant maintained that all the requested information is already in the public domain because ASBOs are made in public and are supposed to be publicly known about (therefore the information should not be withheld). He also pointed to the fact that details of individuals who are the subject of ASBOs can be specifically published by councils if they so wish.

14. The first data protection principle requires that:

*'Personal data shall be processed fairly and lawfully, and, in particular, shall not be processed unless –
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.'*

15. The second data protection principle requires that:

'Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.'

16. The key question raised by this complaint is whether disclosure of personal data would be fair and compatible with the purposes for which it was obtained. This question raises various issues including the nature and purposes of ASBOs, policy and practice relating to ASBO publicity, the expectations of the community and the expectations and human rights of ASBO recipients.

17. The Commissioner has drawn heavily on the most recent Home Office Guidance on ASBOs.

18. Chapter 15 of that guidance deals with “Promoting awareness of orders” and itself draws upon the judgment of Lord Justice Kennedy, presiding judge in the case of *R (on application of Stanley, Marshall and Kelly) v Commissioner of Police for the Metropolis and Chief Executive of London Borough of Brent* [2004] EWHC 2229 (Admin), commonly referred to as *Stanley v Brent*.
19. The chapter concentrates on decisions to publicise ASBOs and contains helpful material on the principles to be adopted, the benefits of publicity, the decision to publish, the decision-making process, the content, tone and distribution of publicity and human rights and data protection considerations.
20. Key points which the Commissioner considers to be of particular relevance to his decision include:
 - An effective media strategy is considered “essential” to fulfil the protective purposes of ASBOs.
 - An effective local publicity strategy should increase community confidence in reporting anti-social behaviour, deter potential offenders and ensure that the local population is aware of orders.
 - “Obtaining the order is only part of the process; its effectiveness will normally depend on people knowing about the order.”
 - An individual who is subject to the order should understand that the community is likely to learn about it.
 - Publicity should be necessary to achieve an identified aim such as notifying the public that an order has been made, reassuring the public that action has been taken, notifying the public so they can help in the enforcement of a specific order or to act as a deterrent to others.
 - There is no intention of “naming and shaming” – ASBOs are intended to protect communities, not punish or embarrass individuals.
 - The intended audience should be primarily within the area that suffered and/or covered by the terms of the order.
 - There should be the least possible interference with privacy in order to promote the identified purposes of the ASBO. Any reporting restrictions must be scrupulously adhered to.
 - It will usually be appropriate to issue publicity when a full order is made, rather than an interim order.
21. The balanced nature of the Home Office guidance is summed up in its three concluding principles:
 - A case-by-case approach should be adopted and each individual case should be judged on its merits as to whether or not to publicise the details of an individual who is subject to an order. Publicity should be expected in most cases.
 - It is necessary to balance the human rights of individuals who are subject to orders against those of the community as a whole when considering publicising orders.
 - Publicity should be the norm, not the exception. An individual who is subject to an order should understand that the community is likely to learn about it.

22. The Commissioner acknowledges that the Home Office guidance is focussed on initial publicity and that its emphasis is more on “local” publicity than disclosure to the wider public at large. Nevertheless, the existence and adoption of the guidance will have an impact on expectations and it will have led to case-by-case decisions where publicity (as the norm) will have been sought. Once there has been disclosure to the “local” public domain, it does not seem possible in principle, nor realistic in practice, to attempt any distinction for the wider public domain from which disclosure should be withheld. This reflects the guidance that publicity should be “primarily” within the area, which does not preclude wider coverage and this is expressly contemplated for some cases.
23. The Commissioner therefore believes that it is sensible and appropriate to resolve the data protection questions arising from this complaint by reference to the Home Office guidance. He also takes into account the potentially competing public policies which can be summed up as “community protection” and “open justice” on the one hand and “fairness to wrong-doers” and “rehabilitation” on the other.
24. The fundamental nature of an ASBO is that it serves protective purposes during a finite period. The Commissioner does not consider that disclosure, during its currency, of an ASBO which has already been publicised would amount to breach of the first or second data protection principles. Nor would there be breach in any such case where publicity can be justified in line with the Home Office guidance, even though it was not in fact sought.
25. However, he considers that there would be breach at least of the first principle, where:
- reporting restrictions were imposed by the court at the original ASBO hearing or at any hearing for breach;
 - the ASBO did not proceed beyond interim status;
 - the public authority is satisfied that the ASBO recipient is particularly vulnerable and would be put at real risk by disclosure; or
 - the ASBO has expired.
- There is also likely to be a breach of at least of the first principle where disclosure extends to the identities of victims, witnesses or other third parties.
26. For the avoidance of doubt and having regard to what is said on this point in the Home Office guidance, the Commissioner does not accept that ASBO recipients under 18 are necessarily vulnerable.
27. In applying this approach to the present case, the Commissioner concludes that the Council should not have redacted all the names from the disclosed database but was justified in redacting names in those cases where any of these four exceptions apply or where victims, witnesses or other third parties would be identified.
28. Since the original request was made, some ASBOs which were then current will have expired. The steps to be taken as set out below therefore further exclude disclosure in such cases. In practice, the Commissioner hopes that the Council

and the complainant agree to disclosure of the **current** register of ASBOs subject to redaction where any of the four exceptions apply.

Section 31 (law enforcement)

29. The Council also relied upon section 31 of the Act to withhold the requested information. It maintained that the exemption applied because the information was held in order to enable the following:
- (a) the prevention or detection of crime
 - (b) the apprehension or prosecution of offenders
 - (c) the administration of justice.
30. However, information is only exempt under section 31 if its disclosure would, or would be likely to, *prejudice* situations such as those cited above. In this instance, the Council neither maintained, nor demonstrated that prejudice would result, or would likely result from disclosure. Accordingly, the Commissioner has taken the view that the exemption at section 31 was incorrectly applied by the Council.

The Decision

31. The Commissioner's decision is that the public authority did not deal with the request for information in accordance with the Act.

Steps Required

32. The Commissioner requires the Council to provide the complainant with a copy of its ASBO database but after the redaction of names in those cases where:
- reporting restrictions were imposed by the court at the original ASBO hearing or at any hearing for breach;
 - the ASBO did not proceed beyond interim status;
 - the public authority is satisfied that the ASBO recipient is particularly vulnerable and would be put at real risk by disclosure;
 - the ASBO has now expired; or
 - the names are those of victims, witnesses or other third parties.

Other matters

33. This Decision Notice places weight on disclosure during the currency of an ASBO and makes clear that there should not be disclosure of names where the ASBO has expired. The Commissioner warns that, notwithstanding disclosure during its currency, there would be a breach of at least the first data protection principle if further processing of the disclosed information involved unfairness to an ASBO recipient. For example,

according to the circumstances, wider publication of details of ASBO recipients after the expiry of their ASBO terms could well amount to unfair processing.

Right of Appeal

34. Either party has the right to appeal against this Decision Notice to the Information Tribunal. Information about the appeals process may be obtained from:

Information Tribunal
Arnhem House Support Centre
PO Box 6987
Leicester
LE1 6ZX

Tel: 0845 600 0877
Fax: 0116 249 4253
Email: informationtribunal@dca.gsi.gov.uk

Any Notice of Appeal should be served on the Tribunal within 28 calendar days of the date on which this Decision Notice is served.

Dated the 13th day of February 2007

Signed

**Richard Thomas
Information Commissioner**

**Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF**

Legal Annex

Relevant Statutory Obligations and Provisions under the Act

Section 1(1) provides that -

“Any person making a request for information to a public authority is entitled –

- (a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and
- (b) if that is the case, to have that information communicated to him.”

Section 40 provides that:

40. - *(1) Any information to which a request for information relates is exempt information if it constitutes personal data of which the applicant is the data subject.*

(2) Any information to which a request for information relates is also exempt information if-

- (a) it constitutes personal data which do not fall within subsection (1), and*
- (b) either the first or the second condition below is satisfied.*

(3) The first condition is-

- (a) in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the Data Protection Act 1998, that the disclosure of the information to a member of the public otherwise than under this Act would contravene-*
 - (i) any of the data protection principles, or*
 - (ii) section 10 of that Act (right to prevent processing likely to cause damage or distress), and*
- (b) in any other case, that the disclosure of the information to a member of the public otherwise than under this Act would contravene any of the data protection principles if the exemptions in section 33A(1) of the Data Protection Act 1998 (which relate to manual data held by public authorities) were disregarded.*

(4) The second condition is that by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(c) of that Act (data subject's right of access to personal data).

Section 31(1) of the Act provides that –

“Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice-

- (a) the prevention or detection of crime,
- (b) the apprehension or prosecution of offenders,
- (c) the administration of justice,
- (d) the assessment or collection of any tax or duty or of any imposition of a similar nature,
- (e) the operation of the immigration controls,
- (f) the maintenance of security and good order in prisons or in other institutions where persons are lawfully detained,
- (g) the exercise by any public authority of its functions for any of the purposes specified in subsection (2),
- (h) any civil proceedings which are brought by or on behalf of a public authority and arise out of an investigation conducted, for any of the purposes specified in subsection (2), by or on behalf of the authority by virtue of Her Majesty's prerogative or by virtue of powers conferred by or under an enactment

Section 1(1) of the Data Protection Act 1998 states that:

‘personal data’ means data which relate to a living individual who can be identified –

- (a) from those data or*
- (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller*

The first data protection principle states that:

1. Personal data shall be processed fairly and lawfully and in particular shall not be processed unless-

- (a) at least one of the conditions in Schedule 2 is met and*
- (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*

The second data protection principle states that:

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes