IN THE FIRST-TIER TRIBUNAL **EA/2014/0300 AND 0301**
(GENERAL REGULATORY CHAMBER)
[INFORMATION RIGHTS]

ON APPEAL FROM:

Information Commissioner's Decision Notice: FER0529617
Dated: 4 November 2014
Appellant: LONDON BOROUGH OF HACKNEY
Respondent: THE INFORMATION COMMISSIONER

Information Commissioner's Decision Notice: FER0530573
Dated: 4 November 2014
Appellant: LONDON BOROUGH OF HACKNEY
Respondent: THE INFORMATION COMMISSIONER
Second Respondent: PETER MUDGE

Heard at: FIELD HOUSE
Date of hearing: 12 May 2015

Date of Decision: 19th June 2015

Before
Michael Jones
Annabel Pilling (Judge)
David Wilkinson

Subject matter:
EIR – Regulation 13(1)

Representation:

For the Appellant:	Timothy Pitt-Payne QC
For the Respondent:	Robin Hopkins
For the Second Respondent:	Peter Mudge

Decision

For the reasons given below, the Tribunal refuses the appeals and upholds the Decision Notices dated 4 November 2014.

Reasons for Decision

Introduction

1. These are two appeals by the London Borough of Hackney (the 'Council') against Decision Notices issued by the Information Commissioner (the 'Commissioner') dated 4 November 2014.

2. Each Decision Notice relates to a request made to the Council for information concerning the IP addresses used to submit responses to a consultation exercise run by the Council in respect of the Hackney Marshes Pavilion. In the first case, the request was for the Internet Protocol ('IP') address and date/time of submission for each response submitted to the online consultation questionnaire, and in the second for the IP address used by 7[1] of the respondents to the consultation.

3. The Council refused to disclose the information relying on regulation 13(1) of the Environmental Information Regulations 2004 (the 'EIR') on the basis that the information was personal data and that disclosure would breach one of the data protection principles.

4. The Commissioner investigated complaints by the requestors. He accepted that both requests were for environmental information and therefore governed by the EIR. He concluded that the IP addresses did not constitute personal data. He did not consider separately whether the information about the date or time of the submissions constituted personal data.

[1] In fact, 10 respondents used the same IP address.

5. The Appellant appealed to this Tribunal on 1 December 2014. The Requestor in the first case was not joined as a party; the Requestor in the second case was joined as Second Respondent. Both cases were heard together at an oral hearing on 12 May 2015.

6. The Tribunal was provided in advance of the hearing with an agreed bundle of material and the requested information itself which was not disclosed to the second respondent as to do so would defeat the purpose of the appeal. We were provided with additional authorities on the morning of the hearing.

Legal framework

7. The specific information is not itself of an environmental nature but it is part of a survey which would likely have an impact on the way in which the Council implemented plans that would affect the Hackney marshes. All parties agree that the information would meet the wide definition of environmental information under regulation 2(1)(c) EIR as it is about a measure likely to affect the elements of the environment listed in regulation 2(1)(a). We agree.

8. The EIR bring into effect Council Directive 2003/4/EC on public access to environmental information (the 'Directive'). The EIR creates a duty on public authorities to make environmental information available upon request, subject to certain exceptions, if in all the circumstances of the case the public interest in maintaining the exception outweighs the public interest in disclosing the information. In respect of the personal data of third parties, that is personal data of which the requestor or applicant is not the data subject, regulation 13 (1) provides that a public authority shall not disclose if disclosure would contravene any of the data protection principles, as set out in Schedule 1 of the Data Protection Act 1998 (the "DPA").

The issues for the Tribunal

9. The issues for the Tribunal are as follows:

(i) Is the information requested personal data?

(ii) If it is personal data, would disclosure contravene one of the data protection principles and thus engage the exception in regulation 13(1)?

Is the information personal data?

10. Personal data is defined in section 1(1) of the DPA:

> *"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…"*

11. The parties are in agreement that this definition includes a 'relates to' condition and an 'identification' condition, and that the issue for the Tribunal is whether the 'identification' condition is met.

12. The Council submits that the IP addresses taken alone amount to personal data, and more so in respect of the first request, when coupled with the additional information of date and time of the submission of the response.

13. Article 2(a) of the Directive defines "personal data" as follows:

> *"personal data" shall mean any information relating to an identified or identifiable natural person (a "data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological mental, economic, cultural or social identity.*

14. The Council argues that as the DPA gives effect to the Directive, it should be construed consistently.

15. The Council relies upon the inclusion of identification "in particular by reference to an identification number". We do not agree with the Council's apparent suggestion that an IP address would fall into this definition automatically. An IP address of a particular device is not the same as an identification number from which a person is identifiable such as, for example, a national identity number, a passport number, a driving licence number, an NHS number or a National Insurance number.

16. Recital (26) to the Directive provides:

> *Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person…*

17. The Council submits that respondents to the survey are identifiable from the date and time when they replied to the survey, and the device from which they replied to it. If an individual is identifiable, the information is personal data.

18. The Commissioner submits that the test to be applied is whether in all the circumstances of the case, it is reasonably likely that a living individual could be identified by any person, taking into account all of the means which are reasonably likely to be used to try to make that identification.

19. The Council submits that the Commissioner's approach was incorrect as he considered only whether the public generally would be able to indentify individuals from the requested information, and that he failed to follow his own Guidance to take account of means likely to be used by individuals with a particular reason to make an identification, the so called "motivated intruder". Before us, the Council emphasised that the question whether the requested information constituted personal

data should not be resolved by reference to whether the requestors (or the public generally) could make identification, but by reference to whether individuals would be identifiable if the information were released into the public domain.

20. The Council had not itself identified any individual from the IP address or combination of IP address and date and time of submission of response to the survey. In correspondence with the second respondent, the Council indicated that in analysing the consultation results, it had examined the IP address repetitions and came to the conclusion that this was indicative of a proxy server. The second respondent submits that it must follow that there would be no means of identifying any individual from this IP address. We agree with this submission; the use of a proxy server would act to prevent individuation.

21. We heard evidence from the Council's Consultation Manager who, in agreeing with suggestions put by counsel, told us that the Council could not be sure that this IP address was that of a proxy server, or whether it could be, for example, in the same house with a number of individuals using the same device.

22. The IP addresses were collected simply as a standard part of the software package. In order to decide whether to include in the survey responses submitted from the same IP address the Council would consider a number of other matters, such as the trend of responses, both from that IP address and generally, and whether the inclusion of the responses from the same address would affect the overall result.

23. The Council submitted that there were a number of scenarios under which identification would be possible, either from the IP address alone or from a combination of IP address and date and time of when the survey response was submitted.

24. Firstly, internet access providers, managers of local area networks and internet service providers would be able to identify individuals from

their IP address alone in circumstances where they had kept a log of the IP address given to a particular internet user.

25. Secondly, any person able to access that information would also be able to identify an individual in the same way.

26. Thirdly, any person with access to the same device used by the individual responding to the survey would be able to determine the IP address of the device and could check whether a response had been submitted.

27. Fourthly, the use of geo-location services would enable identification through information about the geographical location to which a particular IP address relates, either alone or in conjunction with the information as to the date and time of the response to the survey.

28. The Council submits that there is support for its position in the Opinion of the Data Protection Working Party on the concept of personal data dated June 2007, and, in particular, to the consideration of dynamic IP addresses. The Council drew our attention to the following extract:

> "*Internet access providers and managers of local area networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically "log" in a file the date, time, duration and dynamic IP address given to the Internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server, In these cases there is no doubt about the fact that one can talk about personal data in the sane of Article 2(a) of the Directive."*

29. The Working Party appear to regard Recital 26 of the Directive as setting the "test" to be applied: "*to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller to by any other person to identify the said person*. It stated that a mere hypothetical possibility to single out

an individual is not enough to consider the person as "identifiable." If, taking into account "all the means likely reasonably to be used by the controller or any other person", that possibility does not exist or is negligible, the person should not be considered as "identifiable" and the information would not be considered personal data. The criterion should take into account all the factors at stake in a particular case, including cost, intended purpose, the way the processing is structured, advantages expected by the controller, interests at stake, and technical failures.

30. The Council appears to concede that the hypothetical and negligible should be excluded but maintains that there is a very low hurdle to be cleared to get beyond that level.

31. We agree with the Commissioner's assessment of the test to be applied: whether in all the circumstances of the case, it is reasonably likely that a living individual could be identified by any person, taking into account all of the means which are reasonably likely to be used to try to make that identification. The assessment must be relevant to the information in hand.

32. We do not consider the "routes" to identification suggested by the Council amount to anything more than very technical or hypothetical possibilities. The Council itself cannot identify an individual from the information it holds. It suggests that the "motivated intruder" could do so through a variety of routes. We are not persuaded that there is any basis to conclude that there would be any such motivation in this particular case involving a small survey for the provision of leisure facilities in a discrete area of London. There is no evidence that this was a particularly contentious issue, locally or nationally, and the results of the survey suggest a high level of support. We reject the Council's suggestion that the attendance of the second respondent at this hearing could be support for its submission that there is a significant level of motivation in some quarters to attempt to identify the individuals who responded to this survey.

33. Evidentially, there is no basis for suggesting that an Internet Service Provider, of its own volition, would seek to link an IP address with a particular individual, or in fact be able to do more than link with a named account holder. In order for this "key" to identification to be released more widely, there would need to be legal permission sought and obtained. Again, we are not persuaded that there is a remote possibility that this would be the case in respect of the requested information.

34. The Council sought to draw support from the Commissioner's issuing of a Monetary Penalty Notice on 9 May 2011 to a solicitor, as the data controller. The solicitor had been acting on behalf of those whose intellectual property rights were being infringed was able to obtain a court order requiring Internet Service Providers to disclose the subscribers of certain IP addresses. He then wrote letters explaining that the individual's computer had been used to access certain material and threatening legal action. The Council submits that the circumstances of the data breach in this case illustrate how IP addresses can be used to obtain information about individuals' names and addresses.

35. May 2011 case supports the Council's assertion that the IP addresses in the appeal now under consideration are personal data. The Council itself concedes that it cannot be sure whether the letters were sent to individuals who were in fact the user or subscriber of the relevant IP address. In issuing the Monetary Penalty Notice the Commissioner did not need to even form a view about the accuracy of the information held. The mischief in the case was the holding of personal data, including the names and addresses of those to whom the letters had been written, without sufficient security to prevent the hacking which took place and thus the disclosure of personal data.

36. It appeared to us that the Council glossed over the significant step involved in the obtaining of the information from the Internet Service Providers, that is, through a court order. The Internet Service

Providers are not able to disclose this information to general enquiries from a member of the public; there are obligations under the DPA and contractually to subscribers.

37. We agree with the Council insofar as accepting that identification could be achieved by accessing information held by Internet Service or Access Providers, but in our view this is only reasonably likely pursuant to law enforcement or national security procedures, or by private parties using civil litigation to obtain access. In the circumstances of this case we are not persuaded that identification through this route is remotely likely.

38. The third scenario advanced by the Council, that of identification by interrogation of the IP address history, is again a mere hypothetical possibility. The IP address could by dynamic or static; it is not possible to tell from the IP address alone. If dynamic, it would be impossible to identify any individual who had some time ago submitted a response to this survey. This scenario could only occur if the IP address was a static address, if someone was motivated to seek out the history and then did further work. We agree with the Commissioner that this is far from reasonably likely.

39. The fourth scenario, that of identification using geo-location services, was not advanced with any force before us; the Council conceding, quite properly in our view, that this would likely be very broad information, for example, 'London'. The level of sophistication of these services is such that there is no reasonable likelihood of identifying an individual by this route.

40. The Council advanced a further 'stand alone' argument before the Tribunal, relying on the decision by the Court of Appeal in *Google Inc v Vidal-Hall and others* [2015] EWCA Civ 311, linking the IP address to a piece of online behaviour, that is, responding to the consultation.

41. The issue for that court was whether the claimants should be permitted to serve proceedings on the Defendant in California. To obtain

permission from the Court, the claimants had to establish, among other matters, that there was a serious issue to be tried on the merits of their claims. While we found the discussion whether it was arguable that Browser-Generated information constituted personal data interesting, we did not accept that this case assists the Council's position in any meaningful way. First, the issue has yet to be decided; the Court of Appeal was considering whether to permit proceedings to be served. Second, the Browser-Generated information is very different from an IP address alone, consisting of detailed browsing histories comprising a number of elements such as the website visited, and dates and times of such visits, and information derived from use of the 'double-click' cookie, which amounts to a unique identifier, enabling the browsing histories to be linked to an individual device/user. The Browser-Generated information could then be processed by Google specifically so as to enable advertising to be targeted at users; this would be revelatory information about an individual and a third party with access to the device could link the information with the user with the result of access to "privacy intrusive" information about that user. We do not consider that we can 'read across' as the Council submits.

42. Taking into account the means reasonably likely to be used, we are not satisfied that it is reasonably likely that a living individual could be identified from the IP address information taken alone, or even in combination with the date and time of submission of the response to the survey. We are therefore satisfied that the information requested is not the personal data of a third party. We do not need to go on to consider whether disclosure would contravene one of the data protection principles.

Conclusion

43. We agree with the Commissioner that the requested information is not personal data and the Council was not entitled to refuse the requests on the basis of regulation 13(1) EIR. We unanimously refuse this appeal.

44. The Council must now disclose the information or issue a valid refusal notice which does not rely on section 13.

19th June 2015