FIRST DIVISION, INNER HOUSE, COURT OF SESSION

[2010] CSIH 43

XA51/09

OPINION OF THE COURT

delivered by THE LORD PRESIDENT

in Appeal by

CRAIGDALE HOUSING ASSOCIATION AND OTHERS

Appellants;

against

THE SCOTTISH INFORMATION COMMISSIONER

Respondent:

Lord President

Lord Wheatley

Lord Kinclaven

_____

Act: J J Mitchell, Q.C., O'Carroll; Anderson Fyfe LLP

Alt: Johnston, Q.C., Munro; Anderson Strathern LLP

Non participating party: The Chief Constable, Strathclyde Police; Simpson & Marwick

19 May 2010

Introduction

[1] The appellants are all housing associations in Strathclyde. In 2007 they each made a request for information from the Chief Constable of Strathclyde Police ("the Chief Constable"). The Chief Constable, who is a Scottish public authority within the meaning of the Freedom of Information (Scotland) Act 2002 ("the 2002 Act"), holds information - no doubt detailed information - about registered sex offenders ("RSOs") residing in his police area. The information requested was in each case statistical information about the number of registered sex offenders living in certain postcode districts, specified to the fourth postcode digit, within the Greater Glasgow area. The populations in each of these districts vary from around four to over ten thousand - with one exception where the population is under one thousand. The districts fall into two categories: those in which the appellants' tenants reside and those which the appellants consider to be more affluent districts. The stated purpose of the requests was to ascertain whether the former group was carrying a greater burden as regards housing registered sex offenders than the latter. The Chief Constable refused each request, relying on a number of exemptions contained in the 2002 Act. Applications for review of these decisions by the Chief Constable also having been refused, the appellants applied to the respondent under section 47(1) of the 2002 Act. On 16 February 2009 the respondent, having considered the cases together in a single investigation, issued a decision in which he held that the Chief Constable had acted in compliance with Part I of the 2002 Act. In terms of section 56 of that Act the appellants now appeal against that decision.

While the Chief Constable is also a respondent in this appeal, no argument was presented on his behalf before us.

Legislative Framework

[2] Under section 1 of the 2002 Act a person who requests information from a Scottish public authority is entitled to obtain it, subject to certain absolute exemptions, one of which is to be found at section 38 of the Act, which provides *inter alia*:

"(1) Information is exempt information if it constitutes -

...

(b) personal data and either the condition mentioned in subsection (2) (the "first condition") or that mentioned in subsection (3) (the "second condition") is satisfied ...

(2) 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 (c.29), 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".

The appellants accept that if the statistics which they requested were personal data, absent the consent of the offenders to whom they relate, their disclosure would contravene the data protection principles relating to sensitive personal data. The issue in the present appeal is accordingly whether they do constitute personal data. Section 38 (5) provides that the definition of that term is to be found at section 1 of the Data Protection Act 1998 ("the 1998 Act"), which states, *inter alia*:

"'data controller' means ... a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed; ...

'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 1998 Act was enacted primarily to implement Directive 95/46/EC which by Article 2 defined "personal data" as meaning "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, ...". 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 said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable ...".

The respondent's decision

[3] In his decision the respondent acknowledged that, viewed in isolation, the information requested "appears to be truly anonymous, in that it does not permit identification of any individual RSO represented by the statistics" (para 42). However, he considered that it was necessary to consider the statistics in conjunction with other information in the public domain, including all the means likely to be used by a determined person with a particular reason to make an identification (paras 43 - 44). In doing so, he referred to guidance issued by the UK Information Commissioner (*Data Protection Technical Guidance - Determining what is personal data, 21 August 2007*). He also took into account information which he had received from Strathclyde Police about determined efforts being made by members of the public to identify RSOs, some leading to assaults, including in one case the murder of someone who was mistakenly identified as an RSO, as well as guidance issued by the Office for National Statistics (*Review of the Dissemination of Health Statistics: Confidentiality Guidance, 2006*) and the United Kingdom Association of Cancer Registries (*Guidelines on release of a) individual level anonymised information and b) tabular information based on small populations or small cell counts (potentially identifiable information)*) regarding the risks of identification in disclosing data. He concluded that the geographical and population size of the postcode districts meant it was unsafe to release the statistics and that there was a risk of identification where they were combined with other publicly available information (paras 49 - 54). This process of reasoning is examined in more detail later.

Submissions on behalf of the appellants

[4] Mr Mitchell presented two related main grounds of appeal: first, the respondent had erred in concluding that the statistics sought were personal data in terms of the 1998 Act; secondly, in considering the central issue of identification, his fallacy was to assume that disclosure to the appellants would place the statistics in the public domain. The respondent's answers to the first ground of appeal, and correspondence from Strathclyde Police to which we were referred, also hinted at a "hard-line" approach: the Chief Constable, as the "data controller", retained the raw (detailed) data from which the statistics requested would be compiled; those statistics, however generalised, when combined with that raw data could result in an identification and were thus "personal data" (cf paragraph (b) of the definition). On that hypothesis, however, it would never be possible lawfully to disclose redacted or anonymised information unless in the unlikely event of the data controller destroying the raw data in such a way that he could not retrieve it. Moreover, the respondent had authorised the release of similar statistics in previous decisions involving larger geographical areas. He had distinguished them on the basis that they involved no risk of identification. That, it was submitted, was the real issue in the present case. The genesis of the 1998 Act was Directive 95/46/EC, the broad purpose of which was illuminated by its Recitals. While Recital (26) indicated that the principle of protection applied to information concerning an identified or identifiable person, it also stated that it did not apply to data which had been rendered anonymous.

[5] The respondent's decision in effect correctly acknowledged that, viewed in isolation, the statistics requested were anonymous. His error was then to address the likelihood of people other than the appellants making an identification. The guidance issued by the UK Information Commission cited as an example of a determined individual, among others, an industrial spy. That was an absurd standard to apply and took no account of the actual applicant's motives. In that regard, in principle, the appellants were willing to provide an undertaking not to disclose the data further. If releasing the information to the appellants in effect placed it in the public domain, the third ground of appeal was that the respondent's decision did not elucidate properly the "other factors" which might lead to identification (para 49 of his decision). He seemed to rely on the attitude of some members of the public, including some members of the communities covered by the requests, towards registered sex offenders (paras 52 and 54). The data sought would provide no assistance in any attempts at identification. When one looked at the guidance issued by the Office for National Statistics and the United Kingdom Association of Cancer Registries, it was not clear how they supported the conclusion that the population number and geographical size of the areas made it unsafe to release the statistics, particularly where identifying features of the offenders such as age or gender had not been requested.

[6] In support of his submissions, Mr Mitchell referred to *Common Services Agency* v *Scottish Information Commissioner* 2008 SC (HL) 184. He relied principally on the approach adopted by Baroness Hale of Richmond: if neither the recipient, nor anyone else to whom he might pass the data on, could identify individuals from the statistics themselves, they would not be personal data, the recipient not having access to the raw data from which they were compiled (para [92]). That was consistent with the policy considerations in Recital (26) of the Directive. It required the definition of "personal data" in the 1998 Act to be read purposively, so that for the purpose of processing by disclosure regard had to be had to the means of identification available to the recipient. Alternatively, on Lord Hope of Craighead's approach, both the data disclosed and the other information held by the data controller had to contribute to any identification in terms of paragraph (b) of the definition of "personal data": if the statistics were truly anonymised they would make no contribution, thus taking them outside the scope of the 1998 Act (paras [23] - [28]). That approach had been adopted in argument by the UK Information Commissioner before the Information Tribunal (*Department of Health* v *The Information Commissioner* EA/2008/0074 15 October 2009, at paras 37 -38). In contrast, Lord Rodger of Earlsferry considered that the "other information" referred to in paragraph (b) did not include other data held by the data controller, the question being whether, in terms of paragraph (a), an individual could be identified from the data requested (paras [75] - [78]). There was a certain strain to that approach, but it also permitted the disclosure of anonymised data. In each of the approaches one looked only at the statistics requested to determine if they amounted to personal data. This supported grounds 1 and 2. Moreover, the unanimous decision of the House had been to remit the case to the respondent for him to consider whether the statistics requested could be rendered anonymous. That confirmed that it was theoretically possible for such information to be disclosed, undermining the "hard-line" approach.

[7] Mr Mitchell submitted that the respondent had erred in law and that the court should remit the case back to him or allow the appeal *de plano* and order disclosure.

Submissions on behalf of the respondent

[8] Mr Johnston confirmed that the dispute between the parties concerned whether the information requested was personal data. Generally, there was no presumption in favour of disclosure (*Common Services Agency* v *Scottish Information Commissioner*, per Lord Hope at paras [4] and [7]). The question had to be considered in light of the underlying Directive (*Common Services Agency* v *Scottish Information Commissioner* per Lord Hope at para [20] and Lord Rodger at para [82]). Assistance in understanding the operative terms of the Directive was provided by Recital (26) (*Craies on Legislation*, 8th ed, paras 32.5.1 -32.5.3; *Interinstitutional Agreement of December 22, 1998 on Common Guidelines for the Quality of Drafting of Community Legislation* OJC 73 (printed as an appendix to *Craies*), at para 10). It suggested a broad approach, with all means likely reasonably to be used by a determined person to identify an individual being taken into account. While member states had a margin of appreciation as regards its implementation, the Directive had a clear objective, namely the protection of individuals' fundamental right to privacy from direct or indirect identification (Articles 1 and 2). The appellants' approach of considering only the data which were disclosed was impractical and flew in the face of that objective.

[9] The assessment of what was personal data had to be made prior to its disclosure and was not tested by the motives or knowledge of the particular would-be recipient (*Common Services Agency* v *Scottish Information Commissioner*, per Lord Hope at paras [26] - [27] and Lord Rodger at para [80]). The appellants' approach required too much to be read into the 1998 Act and did not take account of the different forms of "processing" data, such as its retention (see section 1 of the 1998 Act). The "hard-line" approach had not been adopted by the respondent, although there was some support for it in *Common Services Agency* v *Scottish Information Commissioner* (Lord Hope at paras [22] and [26] and Lord Rodger at paras [80] - [81]). The question was whether the respondent had correctly adopted a broad approach to identifiability. The effect of disclosure was to place the information in the public domain (*Office of Government Commerce* v *Information Commissioner* [2008] EWHC 774 (Admin) [2009] 3 WLR 627, per Stanley Burnton J at para 72). A purposive approach therefore required a consideration of the information already available in that domain. That was consistent with the guidance issued by the UK Information Commissioner (pages 21 - 22).

As the respondent had no power to restrict the use to which recipients might put any disclosed data, it was unclear how he could seek undertakings from them. If the particular motives of an applicant were relevant, e-mail correspondence from the appellants to the respondent dated 27 and 28 March 2008 suggested that they did wish to place the data in the public domain.

[10] The respondent had been correct in his approach. When read as a whole, his decision did not suggest that the data requested were in fact "truly anonymous" (see para 42). Rather, his conclusion was that the information was not sufficiently anonymised. That was a question of fact for the respondent and his conclusions could not be assailed (*Common Services Agency* v *Scottish Information Commissioner*, per Lord Hope at para [27], Lord Rodger at paras [79] and [81] and Baroness Hale at para [90]). In that regard the population and geographical size of the postcode districts were highly relevant factors, distinguishing the present case from others where data had been disclosed. The risk of identification increased where small groups of individuals knew personal details about each other, for example whether someone was in regular contact with the police. The data also potentially set a target within these areas and ran the risk of increased efforts being made at identification. The respondent had recognised that not all sources of additional information could be ascertained but was entitled to take into account the risks highlighted to him by the police. Moreover, standing the legislative framework, not every piece of information upon which he had relied could feature in his decision (cf *Scottish Ministers* v *Scottish Information Commissioner* 2007 SC 330, per Lord President Hamilton at para [18]).

[11] Mr Johnston invited us to refuse the appeal. If, however, the court was minded to grant it, the matter should be remitted to the respondent for consideration of the other exemptions relied on by the Chief Constable (see paragraph 72 of the respondent's decision).

Reply by Mr Mitchell

[12] Standing Mr Johnston's submissions, the appellants accepted that, if they were successful, the case should be remitted to the respondent for further consideration. Mr Mitchell referred to statistics, which were not accepted as accurate by the respondent, outlining the overall number of registered sex offenders in Glasgow. RSOs could not readily be identified from their attendance at police stations as that only happened rarely. The respondent had submitted that what constituted personal data depended on the information available to the data controller, whom he did not accept was the would-be recipient. If that were correct, the question was determined solely by information in the hands of the Chief Constable, it being irrelevant what other relevant information was available to anyone else. That unattractive proposition would not arise on Lady Hale's approach. The respondent's decision clearly recognised that, in isolation, the statistics were anonymous (paragraph 42). It was self-evident that these alone could not permit identification. The respondent had failed adequately to explain how, with information otherwise available, identification could be made.

Discussion - "personal data"

[13] The definition of personal data as provided in the 1998 Act and adopted by reference in the 2002 Act (section 38(5)) has given rise to some difficulty. The House of Lords wrestled with that issue in *Common Services Agency* v *Scottish Information Commissioner*. Three quite different approaches can be detected, expressed by Lord Hope, Lord Rodger and Lady Hale respectively. Lord Hoffmann agreed comprehensively with Lord Hope. Lord Mance addressed the "rival views" of Lord Hope and Lord Rodger (but not that of Lady Hale), concluding (para [97]) that it was unnecessary in that case to decide between the two views referred to, adding "but my own preference is for Lord Hope's".

[14] Although Lady Hale's approach is unsupported by any of the remainder of their Lordships, Mr Mitchell founded primarily on that approach, though, he said, he could "live with" Lord Hope's.

[15] The difficulty arises primarily in the interpretation of element (b) in the definition of personal data, as that definition is to be applied in the context of the 2002 Act. That context is of disclosure of information or

data. Disclosure is only one of the modes of "processing" in relation to information or data (1998 Act, section 1(1)). Other modes include organisation, retrieval and use. The purpose of element (b) is more readily comprehensible in the context of such other modes.

[16] In *Common Services Agency* v *Scottish Information Commissioner* Lady Hale stated at para [91]:

"We would all like the legal position to be that, if the risk of identification can indeed be eliminated, the Agency [the data controller in that case] is obliged to provide [the information]. That reflects the expectation in Recital 26 of the European Directive 95/46/EC: that the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. It would have been so much easier if this had been clearly stated in the Data Protection Act 1998."

She then added (para [92]):

"Much though I would like that to be the position, I have had much more difficulty in spelling it out from the definition of 'personal data' in section 1(1) of the Act. In the end, however, I have reached it by the following route. For this purpose, I am assuming the particular data which Mr Collie has requested, anonymised in such a way that neither he nor anyone else to whom he might pass them on could identify the individuals to whom they relate. The Agency may well have the key which links those data back to the individual patients. The Agency therefore could identify them and remains bound by the data protection principles when processing the data internally. But the recipient of the information will not be able to identify the individuals either from the data themselves, or from the data plus any other information held by the Agency, because the recipient will not have access to that other information. For the purpose of this particular act of processing, therefore, which is disclosure of these data in this form to these people, no living individual to whom they relate is identifiable. I am afraid that this may not be exactly the same route as that taken by either of my noble and learned friends, Lord Hope of Craighead or Lord Rodger of Earlsferry, but for practical purposes this may not matter and I have no wish to add further confusion to this already confusing case by elaborating."

[17] Lady Hale's route may be described as purposive, or even adventurous. But it does not, in our view, assist the appellants in this case. She concentrates on the "recipient" (rather than the person holding the data) and on that person's capacity to identify individuals. But there is nothing to suggest that she had in mind only the immediate recipient. She indeed speaks of the particular data being "anonymised in such a way that neither he nor anyone to whom he might pass them on could identify the individuals to whom they relate" (emphasis added). There is nothing in the 1998 Act nor in the 2002 Act (or at least nothing to which our attention was drawn) which prohibits an immediate recipient of personal data from passing that data on to others. (We disregard for present purposes any restriction which might arise from a particular immediate recipient being himself a data controller.) There is nothing to suggest that the purpose or intention (or the supposed purpose or intention) of the person requesting the data has any part to play in whether the data in question are or are not personal data. If data are released under the 2002 Act, they are then available at large. We agree with the observation made by Stanley Burnton J (in the context of the equivalent United Kingdom legislation) in *Office of Government Commerce* v *Information Commissioner* at para 72, where he said:

"Disclosure under FOIA is always to the person making the request under section 1. However, once such a request has been complied with by disclosure to the applicant, the information is in the public domain. It ceases to be protected by any confidentiality it had prior to disclosure. This underlines the need for exemptions from disclosure."

[18] The central challenge by the appellants to the respondent's position on this aspect (namely, that the respondent was in error in maintaining that release to the appellants would put the statistics in the public domain) is accordingly, in our view, unsound and must be rejected. We should add that, in any event, it is apparent from the papers before us that the appellants in making the request had no intention of keeping knowledge of the statistics in question, if released, to themselves; their very purpose was to use them for the legitimate but public purpose of advancing their contention that certain districts had a disproportionate number of RSOs living in them.

[19] In these circumstances it is unnecessary to examine the approaches of Lord Hope or Lord Rodger to the interpretation of "personal data". Neither approach supports the appellants' contention. Nor is it necessary to say anything about the "hard-line" approach, under which, on a strict interpretation of the domestic legislation, anonymised information could not be released unless the data controller at the same time destroyed the raw material from which the anonymisation was made (and any means of retrieving that material), other than to observe that it is hardly consistent with Recital (26) to the Directive.

[20] For these reasons the appellants' first and second grounds of appeal (which are inter-related) must be rejected.

Ground 3

[21] Their third ground of appeal is directed against the respondent's process of reasoning (in so far as disclosed by his decision) leading to his decision that the data in question were personal data by reason of the identifiability of living individuals from the statistics as used in the context of other facts available in the public domain. At para 42 the respondent said:

"The information which would be provided by disclosure of the statistics consists of two elements: the postcode sector defining the geographical area covered by the request and the number of RSOs living within that area. If this information is viewed in isolation it appears to be truly anonymous, in that it does not permit identification of any individual RSO represented by the statistics."

[22] At para 43 he added:

"However, it is not sufficient to look at the statistics on their own. The Commissioner must consider the likelihood of identification. This will include a consideration of the population and geographical size of the postcode areas in question (generally speaking, the smaller the population and geographical size, the higher the likelihood that identification will occur) as well as what other information is already in the public domain which, together with the disclosure of the statistics, could lead to identification of the RSOs involved. In this regard, the Commissioner must again have regard to recital 26 to EU Directive 95/46/EC, which states that in determining whether a person is identifiable, account should be taken of all the means likely, reasonabl[y] to be used by any person to identify the person."

[23] That reasoning is clearly correct. The statistics in themselves are incapable of identifying any individual. They would presumably disclose, in relation to each postal district, either that there were no RSOs living in it or that a positive number were so living; we were informed that in no case would any positive number for any district exceed 100, though it might be less than 10.

[24] In para 44 the respondent observed that it should be assumed that it is not just the means reasonably likely to be used by the ordinary man on the street to identify a person, but also the means which are likely to be used by a determined person with a particular reason to want to identify the individual. We agree with that observation. The illustration of an industrial spy may be somewhat colourful but using the touchstone of, say, an investigative journalist would not be extravagant.

[25] In the succeeding paragraphs the respondent sets out why he has come to the conclusion (at para 54) that living individuals can be identified from disclosure of the data and that these data are accordingly personal data. It is appropriate to set out in full the relative paragraphs. These are:

"45. Although the Housing Associations have made it clear that they do not wish to know the identities of the individuals covered by their requests, Strathclyde Police have provided the Commissioner with examples of determined efforts being made by members of the public to identify RSOs living in some of the areas covered by the Housing Association requests.

46. The Police also provided examples relating to the wider Strathclyde Police area and through other parts of the UK. There are examples of identification leading to assault and, in one particularly unhappy case, of a

murder of someone who was mistakenly identified as an RSO.

47. The Commissioner has considered the question of identifiability from several angles. He has looked at the guidance adopted by other organisations for the 'safe' (i.e. truly anonymous) disclosure of statistics relating to sensitive personal data and has considered that guidance in the light of the case before him. He has also looked at the range of information potentially available to the public about the individuals represented by the statistics. He has also looked at the information Strathclyde Police have provided about local circumstances for some of the areas covered by the Housing Associations' requests, and considered whether any of this information was relevant in assessing whether disclosure of the RSO statistics would lead to identification of individuals.

48. The Office for National Statistics (ONS) has issued guidance on preserving confidentiality in relation to the dissemination of health statistics; and the United Kingdom Association of Cancer Registries (UKACR) has issued guidance on the disclosure of potentially identifiable information. While he is not bound by such guidance, the Commissioner acknowledges the expertise acquired by both bodies in the dissemination of statistics drawn from sensitive personal data and has found this guidance useful in coming to a decision in the current case.

49. The Commissioner has drawn the following conclusions from reading the guidance:

- The geographical and population size of the postcode sectors involved here are considerably smaller than the size deemed 'safe' by ONS or UKACR, in relation to cell counts of 1 or 2.

- The geographical or population size of the sample is not necessarily the only criteria to consider in establishing whether anonymity would be preserved following disclosure; other factors may come into play.

- There may be a risk of identification through 'matching' or linking with data from other source of publicly available information.

50. This strongly suggests to the Commissioner that sensitive personal data would not normally be released at the level involved here because of the likelihood that disclosure would lead to identification. It is also worth noting that while the actual population size may be considerably smaller than the size usually deemed 'safe', given that the statistics relate to RSOs (a high percentage of whom will be male, and over a certain age), the actual number of people generally considered to fall within the category of possible RSOs will be further reduced.

51. The Commissioner also considered whether any additional information is generally available which might lead to identification of individuals represented by the statistics. He found that media reports of the trial or release of RSOs can indicate the individual offender's home area, although in such cases the location was usually described in broader terms than the area covered by the postcode sector. However, the Commissioner found one case where the destination address of a released RSO was indicated in some detail.

52. The Commissioner is also aware that information (and hearsay) may circulate within a community in more informal ways. As noted above, Strathclyde Police has provided the Commissioner with evidence that in some of the communities covered by the requests, residents have made active attempts to discover the identity of sex offenders living in their midst, or have taken the opportunity presented by a public meeting to voice strong opposition to sex offenders being housed in the local area.

53. It is not possible to ascertain all additional sources of information which might be used in combination with the RSO statistics by a person determined to identify the individual offender(s) in a given postcode sector. The Commissioner accepts that such additional information may serve only to strengthen suspicion rather than positively confirm the identities of those individuals. However, given the subject matter of the statistics, there is also an increased likelihood that individuals will attempt to identify some of the individuals involved, although the Housing Associations do not agree that this is the case.

54. Having considered the applications from the Housing Associations in some detail, together with the submissions from the Associations as well as from Strathclyde Police, the Commissioner has come to the conclusion that living individuals can be identified from the disclosure of the statistics. He also considers that the information clearly relates to the individuals, given that it is biographical in a significant sense and that it has the individuals as its focus. As such, the Commissioner has come to the conclusion that the statistics are personal data as defined by section 1(1) of the DPA."

[26] A number of matters arise from these paragraphs. First, the respondent records concerns raised by the Chief Constable about determined efforts being made by some persons to identify RSOs and the consequences which may flow from identifications (including false identifications). These are legitimate concerns. It may also be that the release of statistics recording that a specific number of RSOs are resident in a particular postal district may stimulate vigilante individuals or groups of individuals to seek to identify who they are. But these concerns or that stimulus, if it exists, do not explain how, with the aid of the statistics, identification of individual RSOs is more likely.

[27] Secondly, the respondent has considered the approaches to the release of statistical data adopted by other organisations - in particular the office of National Statistics (its Confidentiality Guide on the Dissemination of Health Statistics) and the United Kingdom Association of Cancer Registries (its guidance on release of (a) individual level anonymised information and (b) tabular information based on small populations or small cell counts). In the former document, under the heading "The Motivated Intruder", the authors address the problem of the use by such a person of data in a table "combined with information from local sources". Reference is made to "information likely to be available to third parties". In that context they advise that all cell counts of one or two for certain geographies would be "unsafe". What is, however, of importance is not so much the size of the cell counts but the nature and extent of the local information available from other sources which, when used with the statistics, can lead to identification. In the absence of knowledge of what other local information is likely to be available, it is impossible to gauge what is the risk of individual identification. The latter document is concerned with the publication of "potentially identifiable data" (original emphasis). The concern is with cell counts of less than five but it is plain that the observations are made in the context of statistics involving divisions into forty single sex, 5-year age groups, the total population for each group being in the order of 1,550. The document does not proscribe the publication of potentially identifiable data but advises that these should be scrutinised and approved (or not) by the director of the cancer registries. No doubt such scrutiny would involve taking account of what other information might be available locally.

[28] The respondent does not, in paragraph 49 or elsewhere, explain what "other factors" or "data from another source of publicly available information" he has in mind in relation to the risk of identification of individual RSOs. While we recognise that he may be concerned not to disclose in a potentially public document information which might be made use of by vigilantes, the appellants are, in our view, entitled to be told, at least in general terms, what these other factors or such other data are. Without that, the respondent's decision is unintelligible. The respondent is under no statutory duty to give reasons for his decision and his decision that the data in question are personal data is a conclusion of fact (*Common Services Agency* v *Scottish Information Commissioner*, per Lord Hope at para [27], per Lord Rodger at para [79]). But where the Commissioner does give reasons voluntarily, the court is entitled to review them (*Rooney* v *Strathclyde Joint Police Board* 2009 SC 73 at para [32]). His conclusion is a secondary finding of fact which must intelligibly follow from the primary material. We recognise that the respondent must be circumspect not to disclose information which ought not to be disclosed (and that the ability of the court to supervise the exercise by him of his powers may be circumscribed accordingly) - *Scottish Ministers* v *Scottish Information Commissioner*, at para [18]. But a need for such circumspection does not absolve the respondent from giving intelligible reasons for his decision. A failure to do so will amount to an error in law.

[29] It is not clear from the decision letter why the disclosure of a statistic that in a particular district the number of resident RSOs was four or fourteen or forty would lead to the identification of the individuals in question or what other information when taken with these statistics would reasonably allow for such

identification. That is so albeit that RSOs are likely generally to be male and "over a certain age" - though such an offender may be of any age and may include boys and youths.

[30] We are not persuaded that in the remaining paragraphs of his reasoning the respondent intelligibly explains his decision.

[31] We should add that in the course of the hearing it was suggested that an identifying factor might be that RSOs would, in accordance with their statutory duty, require to attend a police station and that such attendance might become known in the locality. The statutory obligations incumbent on RSOs are to notify certain particulars and annually to confirm any unchanged particulars (Sexual Offences Act 2003, sections 83-85). Some individuals may require to notify travel arrangements (section 86). Such occasional attendances, the purpose of which should not be known otherwise than to the police and to the offender, might present some risk of identification. But it is difficult to see how the disclosure of the number of RSOs, in the relevant postal district, when combined with knowledge of occasional visits by an individual to a local police station, would increase that risk.

Disposal

[32] In these circumstances we shall sustain the appellants' third ground of appeal and remit to the respondent to consider of new his reasons for concluding that the statistics in question are personal data and to consider, in so far as necessary, the other exemptions referred to in para 72 of his decision.