

FOIMan's FOI Inbox

In response to questions from readers, Paul Gibbons, aka FOIMan, considers your most vexed FOI issues — including the necessity of publishing an email address that requesters can use to submit FOI requests. Paul is a Member of the Examination Board for the Practitioner Certificate in Freedom of Information (www.foiqualification.com)

Welcome to the first of what I hope will become a semi-regular feature in *Freedom of Information*. In the last edition of the journal, I highlighted the fact that even the most informed practitioners don't have an answer for every problem that can cross their desk. Ever ready to help out, I requested that readers send in their questions about the Freedom of Information Act ('FOIA') or Environmental Information Regulations ('EIRs') in the hope that I might be able to put forward my own solutions to their confounding conundrums.

Well, a total of three enquiries poured into my FOI inbox this month. That gives us the opportunity to launch this experiment in interactivity, so I will do my utmost and hopefully more of you will be inspired to run your trickiest questions past me in future issues.

In this article, we will first look at when statistics become personal data — and why the number five won't always be relevant. A more practical question comes next, examining the necessity of publishing an email address that can be used to submit FOI requests. The perennial problem of understanding when information is held when public services are provided by private companies will draw matters to a close.

A small problem

Gillian McCaa of Dumfries and Galloway Council wrote to me to ask when it is appropriate to refuse to provide figures of less than five when answering a request for statistics. Whether subject to the Freedom of Information Act (FOIA) or the Freedom of Information (Scotland) Act (FOISA) as Gillian's authority is, this is a problem encountered regularly by practitioners.

The accepted practice is that where a request is for statistics relating to, for example, services provided to a particular demographic group, then there is a risk that if the resulting numbers are very small — let's say only one person in a small town has accessed that service — anyone with access to that fact would be able to put it together with other information in the public domain to identify that one person. Over the years, statisticians have come up with a rule of thumb to address this risk. This rule of thumb is that figures of five or less should be sup-

pressed — usually by rounding those figures up or down.

Since the advent of FOIA and FOISA, FOI Officers, often guided by statisticians in their own organisations, have commonly applied this rule when releasing statistics. This informal rule has only been made more attractive by (often misleading) publicity surrounding the introduction of new data protection laws. Busy practitioners fear accidentally disclosing personal data, but have limited time to understand the actual risks involved. A simple rule of thumb is very appealing in these circumstances.

Needless to say, the practice leaves many requesters frustrated when actual figures aren't provided. If they are conducting research, whether for an article or an academic study, then it can make the data unusable if figures are rounded up or down. When they make complaints to the relevant Information Commissioner, they are often successful.

In their defence, FOI practitioners or their colleagues will often point to official bodies like the Office for National Statistics ('ONS') as the source of the rule. Yet the ONS itself has been moving away from routine suppression of values of five or less for well over a decade. Its modern guidance recommends a more nuanced approach.

So how should practitioners approach the disclosure of statistics if there are concerns about disclosing personal data?

The answer can be found by examining decision notices. Both Information Commissioners are consistent on this issue, so it doesn't really matter whose, but as Gillian is based in Scotland, let's take a look at a decision of the Scottish Information Commissioner.

Decision 019/2019: Ms R and Lothian Health Board (copy at www.pdpjournals.com/docs/887986) relates to a request to a Scottish health body for the number of operations cancelled for non-clinical reasons broken down by cause. In responding to the request, NHS Lothian had refused to provide the figures of five or less, citing the personal data exemption at section 38(1)(b) FOISA. The Scottish Commissioner's decision sets out the approach that the SIC's Office would expect public authorities to follow if they seek to refuse

access to low numbers when responding to FOI requests.

The exemption at section 38(1)(b) FOISA covers the same ground as that at section 40(2) FOIA, namely personal data. Since the exemption only covers personal data, the first step is to confirm whether the lower numbers meet the definition of personal data.

The definition of personal data is set out at section 3(2) of the Data Protection Act 2018: 'any information relating to an identified or identifiable living individual'. The question to be considered then is whether an individual could be identified if numbers less than five were disclosed. The Commissioner summarises the correct test when considering this, based on the European Court's ruling in *Breyer v Bundesrepublik Deutschland* (C-582/14):

'The correct test to consider is whether there is a realistic prospect of someone being identified. When making that

determination, account can be taken of information in the hands of a third party. However, there must be a realistic causal chain — if the risk of identification is insignificant, the information will not be personal data.'

The Scottish Commissioner concluded in the case that there was not a realistic prospect of someone being identified from the numbers suppressed by NHS Lothian. Lothian was unable to show how individuals could be identified. This isn't saying that numbers of less than five should never be withheld; simply that an authority has to be able to explain how the individuals could be identified.

In another case, (Decision 154/2018: Mr D and Fife Council, copy at

www.pdpjournals.com/docs/887987) the council concerned was able to explain the means by which an individual could be identified, with the result that the Commissioner upheld the Council's use of the exemption.

—
"The bottom line is that numbers of five or less cannot automatically be withheld, though they might prompt practitioners to investigate any potential risk. If a case is appealed, regulators will expect to see convincing evidence that the disclosure could realistically lead to individuals being identified."
 —

As mentioned, when the UK Commissioner looks at these cases, she tends to reach similar conclusions (see for example, FS50809007, www.pdpjournals.com/docs/887988 — a recent decision in relation to the Crown Prosecution Service). In seeking to establish whether individuals are identifiable though, the decisions specifically refer to the Information Commissioners Office's own guidance, the Code of Practice on Anonymisation ('the Code'). The Code suggests that in trying to establish whether individuals are identifiable, it is useful to adopt the 'motivated intruder test'. This means considering whether a person could identify individuals using all reasonable means but without any prior knowledge. The Commissioner com-

ments that: 'the motivated intruder test is that if the risk of identification is 'reasonably likely', the information should be regarded as personal data'.

How would a practitioner find out the extent of the risk though? The Code suggests using the following as relevant to establish whether the numbers concerned can be used to identify individuals: search engines; social media; national or local media; the electoral register; local library resources; published data; other FOI disclosures; and genealogy websites.

The ONS publishes useful guidance on intruder testing which sets out a more detailed methodology for motivated intruder tests.

Interestingly, the ICO's Code stresses the difference between certainty and guesswork. The Commissioner's view is that the possibility that someone might be able to guess an individual's identity is not sufficient to make data personal. That being said, practitioners will need to consider whether disclosure could have an impact on individuals' privacy or other rights, even if figures are not strictly personal data. It may be necessary to use other exemptions to protect the statistics if that is the case (and be able to justify doing so).

The bottom line is that numbers of five or less cannot automatically be withheld, though they might prompt practitioners to investigate any potential risk. If a case is appealed, regulators will expect to see convincing evidence that the disclosure could realistically lead to individuals being identified. Practitioners or their colleagues will need to gather that evidence by using techniques reasonably accessible to the public. In some cases that will be more straightforward than in others.

One final note on this. If a public authority discovers how to identify individuals from the data requested, it will often not be sensible to explain it in full to the requester, since this could increase the risk of individuals being identified in the future. However, it will still be important to keep records of the reasoning behind the decision which can be supplied to the relevant Commissioner if necessary. If the regulator is convinced by the argument, they will take similar precautions when publishing their decision if deemed necessary (as for example in Decision 154/2018: Mr D and Fife Council mentioned earlier).

Is it bad form?

The next missive found its way to me from Mark Dobbs of Dorset Healthcare University NHS Foundation Trust. This time it's a question of practicalities.

Mark's Trust has been trying to

(Continued on page 6)

[\(Continued from page 5\)](#)

streamline its FOI processes and wants to encourage prospective applicants to submit their requests via an online form. The Trust would no longer publish an email address, and this is what prompted Mark's enquiry. Volunteers from the FOI request portal site, WhatDoTheyKnow, have told him that this will be in breach of section 8 FOIA. Mark wants to know if they are right.

In short, no. Section 8 FOIA defines a valid FOI request as one which:

- is in writing;
- provides the name of the applicant and an address for correspondence;
- describes the requested information;
- is received in legible form; and
- is capable of being used for subsequent reference.

There is nothing in section 8 — or indeed anywhere in FOIA — which requires an email address to be published for the purpose of facilitating FOI requests. All that section 8 does is establish the validity of submitted requests — however they may be received.

Although the Act remains silent on this issue, it is addressed in the section 45 Code of Practice ('Section 45 Code'). Paragraph 2.3 of the Section 45 Code states that:

'Public authorities should, as a matter of best practice, publish a postal address and email address (*or appropriate online alternative*) to which applicants can send requests for information or for assistance' (my emphasis).

So it is certainly good practice to publish the means by which prospective applicants are encouraged to make requests, but even the Section 45 Code appears to acknowledge that an alternative to an email address — such as an online form — is sufficient.

Nonetheless, the fact that most

public authorities do publish an email address for FOI requesters to use does suggest that doing so is 'best practice' by any usual definition of the phrase. It is also understandable that WhatDoTheyKnow volunteers would be keen to encourage this, since their system requires an email address to which their users' requests can be submitted.

Insisting on the use of an online form, and choosing not to provide an email address for FOI requests to me raises ethical issues. If we accept that access to information held by public authorities is a right, then deliberately limiting the means by which that right can be accessed needs to be properly considered and only done if it can be justified. By refusing to provide an email address for correspondence, it potentially prevents the use of WhatDoTheyKnow to make requests — and a significant proportion of applicants use that medium. It also makes it difficult for anyone who is making so-called 'round robin' requests that are sent to multiple authorities to conduct research using this method, since having to go to each individual website to submit a request is more time-consuming than sending one email to multiple email addresses.

Now I can hear some readers chuckling at this point. 'I don't see the problem,' they'll intone, 'these are exactly the requests that we want to cut down on.' However, whilst these requests may not be the favourites of practitioners or their colleagues, round robin requests in particular often do a great service in identifying public interest stories. It is this kind of request which highlights 'postcode lotteries' when it comes to healthcare or other public services. Journalists and academics use this method to great effect — their round robin requests are amongst the most powerful demonstrations of the value of FOIA. If still not convinced by the ethical aspect though, there is a more practical reason for continuing to publish an email address to which FOI requests should be submitted. If we return to section 8, it does indeed set out the definition of a valid request. It doesn't require public au-

thorities to provide particular means for requests to be submitted.

However, as long as an authority receives a request meeting the requirements of section 8, it will be valid. This means that there is nothing stopping an applicant from handing a piece of paper with their request on to any member of staff, and in principle it will be valid. Equally they can email any member of staff, any board member or elected member of the authority and the request will be valid. The risk is therefore that in the absence of an official FOI email address, potential applicants (or indeed request portals such as WhatDoTheyKnow) will instead decide to send their requests to anyone whose email address is publicly available or can readily be guessed. Are councillors, government ministers or Chief Executives going to thank their FOI Officers if their inboxes are suddenly inundated with hundreds of FOI requests?

In summary, providing an online form for applicants is no bad thing. There's no legal requirement to provide any particular means such as an email address for them to use, but if practitioners want to maintain control over where requests are received, it is a good idea to publish one to complement the online form. Fundamentally, it's a 'good thing' to allow for requests to be submitted via a number of routes, including for that matter old fashioned snail mail.

Contracts and integrated care

Sarah Browne of Pennine Care NHS Foundation Trust writes that: 'In a world of integrated care, it's becoming increasingly difficult to tell who holds the information for the purposes of an FOI. This is made even more difficult when the provider is a private company.' Sarah's absolutely right of course. It's not just in the NHS that the public sector's relationships with business have become complex. This is why there has been extensive debate over extending FOIA to the private sector where it is delivering public services.

Most recently, the government has sought to address this issue by including guidance in the revised Section 45 Code. In particular, at Chapter 9 we are told that the public authority and the contractor should agree at the start which information is held for FOI purposes. It suggests that this should be listed in an Annex or Schedule to the contract.

However, as Sarah points out in her email, this is not always a practical solution since it is not consistently possible to predict what information will result from the contract or what people will want to know. So it will not always be clear who owns information that has been asked for. It will very often be necessary to analyse whether information is held on a case by case basis.

The definition of 'held' is set out at Section 3(2), which states that information is held for FOI purposes if: '(a) it is held by the authority, otherwise than on behalf of another person, or (b) it is held by another person on behalf of the authority.'

It is the latter limb that is relevant for these purposes. Where a practitioner is seeking to establish whether information in the possession of a contractor is held, they are looking at whether the information is held by the contractor on their behalf.

A good illustration of this issue is provided by *Visser v Information Commissioner and London Borough of Southwark* (EA/2012/0125, 11th January 2013). Mr Visser wanted to see an attendance register indicating the attendance of school groups at a leisure centre. He made an FOI request for the register to the council, but the council claimed that it was not held by them, but instead by the private company that ran the leisure centre.

The Commissioner sided with the council, but when the case reached the First-Tier Tribunal ('FTT'), it took a different view. The FTT was particularly influenced by the Upper Tribunal decision of *University of Newcastle v IC and BUAV* [2011] UKUT 185 (AAC). In particular, the UT had commented in that case that: 'there must be an appropriate connection between the information and the authority, so that it can be properly said that the information is held by the authority'. Looking at the contract between the council and the private company, the FTT noted that it required the latter to provide performance information to the council. The FTT concluded that the attendance register existed so that the company could fulfil this obligation. For this reason, it found that the register was held by the council for the purposes of FOIA. Just like our first problem today then, it is going to come down to a 'causal connection'.

If we want to know whether information in the possession of contractors or other private companies is held under FOIA, it will often be necessary to read the small print to establish whether the information concerned has been created to fulfil an obligation to the public authority. If there's a link between a contractual requirement and the information, it will usually be held. Not forgetting of course that 'hold' is an ordinary English word' (the Upper Tribunal again), so in effect, it is a case of 'if in doubt, assume it is FOIAble'.

Conclusion

Thanks to Gillian, Mark and Sarah for these first three entries to my FOI Inbox. I hope the answers have helped a few others beside, and if you have a problem that you'd like me to answer in these pages, please do drop a line to feedback@pdpjournals.com with 'FOI Journal Q&A' in the subject line.

Paul Gibbons

FOI Man

paul@foiman.com

pdp TRAINING

Practitioner Certificate in Freedom of Information

The UK's leading qualification for those working in FOI

The Programme provides full instruction on FOI Law (and the Environmental Information Regulations) and offers practical guidance on the legal requirements, including how to manage an FOI request from inception to completion.

Visit our website to find out more information and to enrol onto the Programme

"I am very pleased to have achieved the Practitioner Certificate in Freedom of Information. The programme provides excellent knowledge and understanding on the practical applications of handling requests for information"
Louise Smith, Financial Ombudsman Service

The Programme modules can be taken on an intensive basis or at different times throughout the year

For more information, go online or contact our training team on +44 (0)207 014 3399



www.foiqualification.com