



**IN THE FIRST-TIER TRIBUNAL  
GENERAL REGULATORY CHAMBER  
[INFORMATION RIGHTS]**

**Case No. EA/2013/0159**

**ON APPEAL FROM:**

**Information Commissioner's  
Decision Notice No: FS50455907  
Dated: 8 July 2013**

**Appellant: GREG CALLUS**

**First Respondent: THE INFORMATION COMMISSIONER**

**Second Respondent: THE HOME OFFICE**

**Heard at: Fleetbank House, 2-6 Salisbury Square, London**

**Date of hearing: 25 February 2014**

**Date of decision: 6 May 2014**

**Before**

**CHRIS RYAN**  
(Judge)

and  
**DAVID WILKINSON**

**Attendances:**

The Appellant appeared in person.  
For the First Respondent: Christopher Knight  
For the Additional Party: Gemma White

**Subject matter:** Whether information held s.1;  
Public interest test s.2;  
Information supplied by, or relating to, bodies dealing with  
security matters s.23;  
Law enforcement s.31;  
Health and safety s.38;  
Personal data s.40

**Cases:** *Corporate Officer of the House of Commons v  
Information Commissioner and others* [2008] EWHC 1084 (Admin).

**IN THE FIRST-TIER TRIBUNAL  
GENERAL REGULATORY CHAMBER**

**Case No. EA/2013/0159**

## **DECISION OF THE FIRST-TIER TRIBUNAL**

The appeal is dismissed.

### **REASONS FOR DECISION**

#### Summary

1. We have decided that (with the exception of one item of information, which came to light shortly before the hearing and has been supplied to the Appellant – see paragraph 26 below) the Home Office did not withhold any information falling within the scope of the Appellant’s original request for information, which was not exempt from disclosure. However, we disagree with the Information Commissioner’s conclusion, in the Decision Notice under review, as to the exemptions that apply to the withheld information. He concluded that the exemption provided under section 23 of the Freedom of Information Act applied. We have allowed the Appellant’s appeal against that part of the Decision Notice but have decided that the Home Office would have been entitled to refuse disclosure on the basis of each of sections 31, 38 and 40.

## The Context of the Appeal

2. The appeal relates to certain investigatory processes which police are permitted to undertake under the Regulation of Investigatory Powers Act 2000 (“RIPA”). In certain specified circumstances the police (as well as other bodies not relevant to this appeal) are entitled to require those operating a postal or telecommunications service (together “Communications Services Providers” or “CSPs”) to disclose information about the sender and recipient of communications (but not the content of those communications) as well as the time when the communication was transmitted or received and the location of those party to the communication at the time. In the Home Office’s Code of Practice on the process it is said that such “Communications Data” embraces “...the ‘who’, ‘when’ and ‘where’ of a communication” but not what was said or written.
3. The process involves an interference with the human rights of those involved in the communications concerned and is therefore regulated to ensure that every instance of such interference is justifiable. One possible justification is that disclosure is necessary for the prevention or detection of crime. A police force may therefore require a CSP to disclose Communications Data only if a “Designated Person” believes that the resulting interference with an individual’s privacy represents a necessary and proportionate response in light of the likely benefit to the investigation or other operation being undertaken. The Designated Person must hold a rank, stipulated by Parliament (currently either an Inspector or Superintendent, depending on the precise nature of the Communications Data being sought) or a more senior officer.
4. In order to obtain authorisation from a Designated Person an investigating officer or other individual seeking Communications Data must complete a detailed written application. The application form is provided, first, to a specially trained individual called the “Single Point of Contact (“SPoC”). A SPoC will have been trained in both the relevant technology and law, so that he/she is able to provide both applicant and Designated Person with advice and assistance on what Communications Data may be obtained and how that may be achieved in both practical and legal terms. The SPoC also plays a role in liaising with any CSPs required to disclose Communications Data. This includes providing assurance that any notice served on it requiring disclosure is authentic and lawful as well as checking the data disclosed. In order to provide comfort to CSPs that the SPoC is the correct person for them to be dealing with, he or she is issued with a Personal Identification Number (“PIN”).

5. Further levels of control are provided by:
  - a. A requirement to appoint a Senior Responsible Officer within the police force (the “SRO”) with responsibility for ensuring the legality and integrity of the relevant processes;
  - b. The existence of the Interception of Communications Commissioner who provides independent oversight of the exercise of the powers and duties contained in RIPA; and
  - c. The availability of a complaints process via the Investigatory Powers Tribunal.

The request for information and the Home Office’s response

6. On 29 March 2012 the Appellant sent the following request for information to the Home Office:

*“I am interested in the identity of Senior Responsible Officers (SROs) and Single Point(s) of Contact (SPoCs) for the purposes of s71 of the Regulation of Investigatory Powers Act (RIPA) 2000 and the Code of Practice for the Investigation of Protected Electronic Information.*

*Please could the Home Office provide me with the following:*

- (a) A list of all current SROs (name and rank) for all police forces in England & Wales*
- (b) A list of all previous SROs (name and rank) for all police forces in England & Wales and the date the (sic) ceased to have this responsibility*
- (c) A list of all current SPoCs (name and rank) for all police forces in England & Wales*
- (d) A list of all previous SPoCs (name and rank) for all police forces in England & Wales and the date they ceased to have this responsibility*
- (e) A list of all current Designated Persons (name and rank) for all police forces in England & Wales*
- (d) A list of all previous Designated Persons (name and rank) for all police forces in England & Wales and the date they ceased to have this responsibility*

*Even if all the information cannot be supplied, I would be grateful for the disclosure of as much of the remainder as is lawful and possible.”*

7. The request was made under section 1 of the Freedom of Information Act 2000 (“FOIA”), which imposes on the public authorities to whom it applies an obligation to disclose requested information unless certain conditions apply or the information falls within one of a number of exemptions set out in FOIA. Each exemption is categorised as either an absolute exemption or a qualified exemption. If an absolute exemption is found to be engaged then the information covered by it may not be disclosed. However, if a qualified exemption is found to be engaged then disclosure may still be required unless, pursuant to FOIA section 2(2)(b):

*“in all the circumstances of the case the public interest in maintaining the exemption outweighs the public interest in disclosing the information*

8. The Home Office responded on 30 April 2012 stating that the identity of current and previous SPoCs, SROs and DPs constituted the personal information of those individuals. Disclosure, it said, would therefore breach data protection principles as set out in the Data Protection Act 1998 (“DPA”) and the information was therefore exempt under FOIA section 40(2), which is an absolute exemption.
9. Following an internal review requested by the Appellant the Home Office maintained its position in respect of section 40(2) but added, in a letter dated 29 May 2012, that the original response should have made it clear that it did not in fact hold information regarding the “rank” of SROs or SPoCs.
10. On 27 September 2012 the Appellant complained to the Information Commissioner about the manner in which his request had been handled. Early in the investigation that resulted the Home Office informed the Information Commissioner (by email of 15 October 2012) that it held a “*database of SPoCs, Designated Persons and SROs who are authorised under RIPA to make decisions regarding information communications data*”. It added that it was seeking clearance from the Office of Security and Counter Terrorism (“OSCT”) and the Association of Chief Police Officers (“ACPO”) for a letter which it intended to send the Information Commissioner with further information. The letter, it said, was likely to include a claim that the Home Office was entitled to rely on an additional exemption, as provided by FOIA section 31(1)(a) (information the disclosure of which would prejudice the prevention or detection of crime), a qualified exemption.

11. On 27 November 2012, after considerable delay and after having been pressed for a response by the Information Commissioner, the Home Office wrote to the Information Commissioner clarifying its position. First, as to the information it held, the letter included this passage:

*"I have investigated further the ownership of the database of SPoCs, DPs and SROs within the Home Office and apologise for any previous confusion caused. The database, known as the SPoC PIN list, is, indeed, owned and held by the Home Office."*

The letter went on to explain that:

- a. The SPoC PIN list included, not only those accredited to perform the role of SPoC, but also some Designated Persons and SROs, who had undertaken the training in order to perform their roles within the RIPA process;
  - b. It was not possible to differentiate between those on the SPoC PIN list who were currently working as SPoCs from those Designated Persons or SROs who had also undertaken the training;
  - c. ACPO would hold a full list of SROs; and
  - d. Each police force would be able to confirm the name of those performing the role of Designated Person within the force.
12. The letter also explained the basis for claiming the exemption under FOIA section 31(1)(a) in respect of Designated Persons, SROs and SPoCs. The claim to the exemption had not been raised at an earlier stage, it was said, because until those dealing with the information request had spoken to "operational colleagues" they had not been aware that disclosure might result in individuals being targeted for direct pressure from criminals.
13. Six weeks later the Home Office wrote again to the Information Commissioner. It stated that, as had been previously indicated to the Information Commissioner informally, it intended to introduce a third claim for exemption. This was FOIA section 23(1) (information supplied by, or relating to, one of a number of security bodies) and was said to be based on the fact that the Intelligence Service and the Serious and Organised Crime Agency each constituted a security body for the purpose of section 23 and were entitled to seek Communications Data under RIPA. The letter went on to reiterate that the Home Office did not hold a list of SROs (current or past) although it might be possible to identify those on the SPoC PIN list who performed that role.

14. On 25 January 2013 the Home Office, writing in response to a request from the Information Commissioner for a final statement of its position, changed its case about the information it held yet again. It stated that, at the date of the information request, the Home Office held a database (called "Outrigger") which contained information about SPoCs within local authorities, the intelligence agencies and some police forces, the information including each individual's PIN number. Separately the National Police Improvement Agency ("NPIA") held a database ("SPoC Book") containing similar information, but for police force SPoCs only.
15. In late 2012 some of the NPIA's functions had been transferred to the Home Office, with the result that it then became owner of both Outrigger and SPoC Book. It had arranged for them to be merged shortly thereafter to form the Communications Data Assistant database. It was only at that point, the letter explained, that the Home Office came to hold a comprehensive list of police force SPoCs. The letter went on to explain, also, that, contrary to what had been said previously, it was not possible to identify SROs or Designated Persons who had attended SPoC training, in order to perform their own roles better, at least without seeking information from individual police forces about those of its officers included in SPoC training attendance lists and the rank each one held.
16. More surprisingly still, the Home Office then changed its position on available exemptions yet again, by adding a claim that the disclosure of the requested information would, or would be likely to, endanger the physical or mental health of an individual or endanger that individual's safety. It was said that the qualified exemption provided by FOIA section 38(1) therefore applied. It also modified the exemption claim previously made under FOIA section 23. Although the Home Office explained the basis of the exemption claim rather cryptically in its letter to the Information Commissioner it provided more detail in a letter to the Appellant dated 14 March 2013, in which it said:

*"Section 23 is being applied in this case as some of the individual SROs, SPoCs or DPS whose details you have requested may have worked alongside, with or in conjunction with any of the security bodies as listed under s.23. If individuals working in any of the police authorities in England or Wales have worked with or had involvement with any of the security bodies listed under s.23 as a part of their job the Home Office would be exempted from providing their details but, in confirming if specific individuals are not exempt under s. 23 we would also be confirming that other individuals have had an*

*involvement with the s.23 bodies, which is why s.23(5) has been used in this response.”*

### The Information Commissioner’s Decision Notice

17. On 8 July 2013, having considered a lengthy submission from the Appellant to the various issues raised by the Home Office, the Information Commissioner issued a Decision Notice in which he concluded that the Home Office had correctly applied FOIA section 23(1) but that it had incorrectly applied section 23(5) in declining either to confirm or deny whether it held any further information beyond that requested by the Appellant. Having decided, on that basis, that requested information was exempt, the Information Commissioner did not proceed to consider the claims to exemption under sections 40, 31 or 38. He did, however, find that the Home Office had breached FOIA section 10(1) and 17(1)(b) in not informing the Appellant, within the 20 working day statutory period, the exemptions on which it relied. He also criticised the Home Office for having provided inaccurate information about the information it held at the time of request although he indicated that, having questioned a Home Office official with detailed knowledge of the department’s Communications Capabilities Development programme and been shown a screen shot of the relevant database, he was satisfied, on the balance of probabilities, that the information held by the Home Office at the time of the information request had been the names of current (and previous) SPoCs, but not their individual rank or status, or the dates when the particular individual may have ceased to perform the role of SPoC.

18. As to the section 23 exemption the Information Commissioner reminded himself that the statutory language was:

*“Information held by a public authority is exempt information if it was directly or indirectly supplied to the public authority by, or related to, any of the bodies specified in subsection 3...”*

He recognised that the bodies specified in subsection 3 did not include any police force and that there was no suggestion that any subsection (3) body had provided the Home Office with the names of SPoCs. Accordingly, he concluded, the exemption would only apply if the information requested could be said to “relate to” one or more of those bodies. The Information Commissioner considered the remit of the Home Office for matters of national security and its consequential involvement with subsection (3) bodies and concluded:



*“29. When the nature of the work undertaken by the Home Office is combined with the close connection between RIPA 2000 and the Section 23(3) bodies, the Commissioner considers that the complainant’s request could be considered to be within the territory of such bodies. That is to say, whilst none of the individual police forces are themselves section 23(3) bodies, it could be reasonably assumed that of all the individuals working within any particular police force, it is those responsible for applying RIPA 2000, who would be most likely to have involvement with section 23(3) bodies...”*

*30. Were it not for the fact that in the context of the complainant’s request, the names of the individuals concerned are indivisible from their RIPA responsibilities, and those responsibilities could reasonably be expected to include involvement with the security bodies, the Commissioner would regard the rationale provided by the Home Office as too remote to establish the required degree of ‘relates to’ between the police individuals concerned and the section 23(3) bodies.”*

19. The Information Commissioner was strengthened in his view that the connection was not too remote by certain additional information provided to him in confidence, which he recorded in a confidential annex to the Decision Notice. We comment on this in our own confidential annex to this decision.

### The Appeal to this Tribunal

20. On 6 August 2013 the Appellant appealed to this Tribunal on the grounds that the Information Commissioner had:
- i. Misconstrued FOIA section 23(1);
  - ii. Relied on evidence that was irrelevant, and insufficient to discharge the burden of proof imposed on the Home Office;
  - iii. Considered evidence on a confidential basis, thus rendering it incapable of challenge; and
  - iv. Failed to come to a decision on the exemptions provided by FOIA sections 40, 38 and 31.
21. Appeals to this Tribunal are governed by FOIA section 58. Under that section we are required to consider whether a Decision Notice issued

by the Information Commissioner is in accordance with the law. We may also consider whether, to the extent that the Decision Notice involved an exercise of discretion by the Information Commissioner, he ought to have exercised his discretion differently. We may, in the process, review any finding of fact on which the notice in question was based. Frequently, as in this case, we find ourselves making our decision on the basis of evidence that is more extensive than that submitted to the Information Commissioner.

22. The Home Office was joined as Second Respondent to the Appeal and each of the Home Office and the Information Commissioner filed a Response to the appeal. The Appellant filed a Reply to both Responses. Directions were given for the preparation of document bundles and the filing of evidence by the Home Office and any other party who wished to rely on oral evidence. Directions were also given for the treatment, as confidential, of certain materials. This resulted in some parts of the appeal hearing having to be conducted in closed sessions.
23. A hearing took place on 25 February 2014. Due to one member of the Tribunal panel being unwell on the day the hearing proceeded, with the consent of all parties, with a judge and one lay member. The Appellant represented himself, the Information Commissioner was represented by Christopher Knight of counsel and the Home Office by Gemma White of counsel.
24. The Home Office had filed witness statements signed, respectively, by Henry Hirsch from the Office of Security and Counter Terrorism at the Home Department and Steve Higgins from the College of Policing. Both witnesses attended the hearing and were cross-examined. We found both witnesses credible and helpful.

*Mr Hirsch's evidence*

25. Background information:
  - a. Mr Hirsch is the lead for all communications data policy in the Home Office and heads a team responsible for the operation of policy in respect of RIPA, including the acquisition and retention of Communications Data and liaison with those within ACPO having responsibilities in that area.
  - b. The detailed operational engagement with SROs, Designated Persons and SPoCs to monitor compliance with RIPA is carried out by ACPO and the Interception of Communications Commissioner, although Mr Hirsch liaises with the Commissioner's office on problems and difficulties that arise in

the course of inspections carried out by the Commissioner's staff.

- c. The acquisition of Communications Data is quite distinct from the interception of communications, being limited to traffic data, service usage data and subscriber data (but not the content of any communications) and is regulated by procedures imposed by RIPA and the Code of Conduct referred to above.
- d. Any request for Communications Data must be routed through a SPoC, who is a trained adviser on the use of such data. A SPoC is accredited and entitled to acquire data from CSPs, and advice should be sought from him or her as part of the application process.
- e. There are approximately 500 law enforcement SPoCs across 43 police forces. They are often not warranted officers, but will be civilian members within the administrative staff of a police force. They may:
  - i. Advise applicants on the acquisition and use of Communications Data, including the data that may be available (and reasonably practicable to acquire) as well as its practical value as proof of wrongdoing;
  - ii. Assist in drawing up the necessary application form, highlighting the data sought and its intended purpose within a particular investigation;
  - iii. Check completed application forms and arrange for their transmission, with his or her comments on legality and/or technical feasibility, to the relevant Designated Person for decision.
- f. Designated Persons will, as mentioned above, hold a senior rank and will be expected to have a current working knowledge of human rights principles, even though there is currently no classroom based learning available that is specifically targeted to the Designated Person role. This is what has led some police forces to send those performing the role of Designated Person on the courses run by the College of Policing for SPoCs.
- g. A SPoC may provide further information requested by a Designated Person before reaching a decision on an application and recording that decision, with reasons, on the original application form.
- h. The whole process of acquiring Communications Data is overseen by a SRO within the relevant police force, who is normally a more senior officer than the Designated Person.

26. Mr Hirsch also explained the handling, with his team, of the Appellant's information request and his state of knowledge, at that stage, of the

information held, including the Outrigger database. He provided detail on the records maintained from time to time, which broadly supported the statements made in correspondence with the Information Commissioner during his investigation (as summarised in paragraphs 10 to 16 above). However, he also disclosed that he had recently discovered that the Home Office held even more information than had come to light during that protracted investigation. This took the form of three files containing names of some people performing the role of SRO at the time (believed to be in 2010). The information was said to have been found during a check of archived material on an electronic filing system during preparations for the hearing of this appeal.

27. In support of the Home Office's claim to exemption under FOIA section 23, Mr Hirsch explained that the acquisition of Communications Data sometimes led on to the interception of communications and other intrusive techniques. Not all of those techniques were available to all police forces and, if a matter reached an appropriate level of severity, it might be passed by the police force to the National Crime Agency or other bodies named in section 23(3). The result, he said, was that some of the individuals identified in the SPoC list would have worked alongside, or in conjunction with, a relevant security body in order to explain what investigative methods had previously been used.
28. Mr Hirsch provided information about the likely salary level of a SPoC and, in the case of those who are officers, the rank (mostly constable or sergeant). He said that, while their identity might become apparent from either the number on their uniform (in the case of a warranted officer) or the evidence they are sometimes required to give in court, the disclosure of a list of names would not have been expected and might put them at risk of duress or attempts to corrupt them at the hands of criminal groups anxious to obtain information about police investigations affecting them. Similarly, he said, foreign governments may seek to corrupt SPoCs, identified from any published list, in order to obtain information on the authorities' capabilities and vulnerabilities in telecoms surveillance. He conceded that approaches of the kind described could be made, in any event, but he highlighted how much easier (and, for the person making the approach, how much less risky) this would be if all relevant names were available on a published list. He explained his fear that this would have a damaging effect on the recruitment and retention of SPoCs. The fact that some SPoCs had apparently self-publicised the role they performed (typically on social media systems), although unwise and to be discouraged, did not significantly alter the overall picture, given the particular circumstances of the few who had done this.

*Mr Higgins' evidence*

29. Mr Higgins is a Metropolitan Police Detective Superintendent with long experience of Communications Data acquisition (including as the SRO for a police force). He is currently seconded to the College of Policing, where he oversees RIPA training for SPoCs and is responsible for the data currently held on the identity of SPoCs. This includes, crucially, the PIN number allocated to each SPoC on completion of training, which provides essential comfort to CSPs that a request for Communications Data emanates from a genuine source and has been properly authorised.
30. The stated purpose of Mr Higgins' evidence was to explain concerns on behalf of the National Policing Data Communications Group, the National Policing Terrorism and Allied Matters, the College of Policing and the Metropolitan Police Service about the possible disclosure of the SPoC list. The result was that parts of the evidence consisted of argument and some of it duplicated information provided by Mr Hirsch. However, relevant facts which emerged were:
- a. A SPoC is likely to have a great deal of information, not available to other police employees, about the personal data a CSP may hold about its customers, the operational capability of police to access Communications Data in order to prevent and detect crime and the progress of sensitive investigations. As the authorised point of contact for any CSP, with appropriate security clearance, a corrupt SPoC could obtain private information. He or she could also provide criminals with valuable information about police capabilities and activities. A number of SPoCs may acquire knowledge of the capabilities of SOCA and the security services, which would be of great value to criminals and terrorists. Making a list of SPoCs available to the public would remove one of the barriers that currently prevent outsiders obtaining that type of information and would expose individual SPoCs to the risk of receiving corrupt approaches using physical threats or blackmail.
  - b. The turnover of police officers undertaking the role of SPoC was significant, with the result that a number on the list will have left the force or moved to other roles. Those roles could include covert operations, anti-terrorism investigations or handling covert human intelligence sources and Mr Higgins considered that, if disclosure were to be ordered, it would be necessary to carry out an operational impact assessment in order to consider the safety of the individual and the integrity of any investigation in which he or she may be involved.

- c. Communications Data is a factor in over 90% of major prosecutions and any reduction in the number of SPoCs, resulting from their unwillingness to continue in the role once their identities had been disclosed, would undermine the task of investigating crimes.
- d. A selection of (unidentified) SPoCs who had been questioned by Mr Higgins all expressed grave concerns about a list of SPoCs becoming freely available, in particular if it subsequently became available on the internet.
- e. Some SPoCs had disclosed on the LinkedIn networking site the role they performed although, on closer examination of the individual entries, only one of those identified was currently performing the role. That individual, upon realising the dangers inherent in this level of disclosure, had removed her profile.
- f. Steps were being taken to ensure that SPoC training in the future covered the dangers of disclosure by self-publication, whether on social networking sites or otherwise.

#### Issues to be determined on the appeal

31. We propose to depart from the order of issues set out in the Grounds of Appeal and to deal with them in this order:

1. Whether the Home Office held information at the date of the request for information, in addition to that which it has said that it held (paragraphs 32 to 35 below). We conclude that (despite the very unsatisfactory manner in which the Home Office searched for information and reported its findings to the Appellant, the Information Commissioner and this Tribunal) the only information falling to be considered is the list of SPoCs, as that is all the relevant information held at the time.
2. Whether FOIA section 23(1) applies to exempt the SPoC list from the obligation of disclosure imposed by FOIA section 1 (paragraphs 36 to 43 below). We find that it does not because the list does not “relate to” any of the security bodies listed in section 23(3). It follows that the “neither confirm nor deny” issue raised before the Information Commissioner under FOIA section 23(5) is not capable of arising.
3. Whether FOIA section 40(2) applies to exempt the SPoC list (on the ground that it represents the personal data of each of the individuals identified) and that disclosure would breach one of the data protection principles (paragraphs 44 to 54 below). We have decided that the SPoC list is exempt under this ground.

Although it is, strictly speaking, not necessary for us to go on to decide whether the SPoC list could have been withheld under any of the other exemptions relied on by the Home Office, we propose to do so as they were each fully debated before us and (in the case of section 31) more obviously applicable to the facts of the case, as those facts eventually emerged from the witness statements summarised above. The further issues are:

4. Whether FOIA section 31 applies to exempt the SPoC list (on the ground that disclosure would be likely to prejudice the prevention or detection of crime) and, if so, whether the public interest in maintaining that exemption outweighs the public interest in disclosure (paragraphs 55 to 57 below). We conclude that the exemption is engaged and that the public interest balance favours maintaining the exemption.
5. Whether FOIA section 38 applies to exempt the SPoC list (on the ground that disclosure would be likely to endanger an individual's health or safety) and, if so, whether the public interest in maintaining that exemption outweighs the public interest in disclosure (paragraphs 58 to 61 below). We conclude that the exemption is engaged and that the public interest balance favours maintaining the exemption.

#### Issue 1: Information Held

32. We have previously mentioned the list of SROs which Mr Hirsch stated in his witness statement had been discovered recently. Following its disclosure, but before the hearing of the appeal, the Home Office disclosed the list to the Appellant. We do not therefore consider it further, except to record that its discovery was the last piece of evidence demonstrating a lamentable approach by the Home Office to the performance of its obligations, under FOIA section 1, to identify relevant information and disclose its existence promptly.
33. The Home Office invited us to accept that, despite what it described in its skeleton argument as a "regrettable lack of clarity at the earlier stages in the process", we should accept that the only information falling within the scope of the request for information, held by it at the date of that request, and not disclosed to the Appellant, was the list of SPoCs. The Information Commissioner supported the argument, particularly in light of the rigour and scope of his own attempts to clarify the position during the course of his investigation.

34. The Appellant, understandably in the circumstances, criticised the approach adopted by both the Home Office and the Information Commissioner and suggested that all the information sought in the original request must have been held, even though not necessarily in a single unit or place, and not necessarily on the Home Office's own behalf. He also criticised the Information Commissioner for having accepted a screen shot showing the data fields of the relevant database and not pursuing his enquiries further. He argued that the conclusion reached should, as a result, be treated as perverse.
35. We have had the benefit of Mr Hirsch's detailed witness statement describing the searches made and explaining why it was necessary for the Home Office to hold information on SPoCs but not either SROs or Delegated Persons. Although the Home Office was found subsequently to have been holding a list of SROs, the nature and likely source of that information was satisfactorily explained. We also observed Mr Hirsch answering questions. We are satisfied that the Information Commissioner's investigation and Mr Hirsch's further searches before the hearing together demonstrate that, on the balance of probabilities, the Home Office did not hold any further relevant information at the time when it received the Appellant's information request.

#### Issue 2: SPoC List exempt under FOIA section 23?

36. We have set out the relevant statutory language in paragraph 18 above. The parties agreed that the police authorities were not included among the list of security bodies in section 23(3) and that the only issue was therefore whether the SPoC list "related to" one of those listed bodies.
37. The Appellant argued, first, that the Information Commissioner fell into error by construing section 23(1) without any reference to section 24 (which provides that information which does not fall within section 23 is exempt information if exemption from the obligation to disclose is required for the purpose of safeguarding national security). He argued that the broader the scope given to the absolute exemption provided for under section 23(1) the narrower the ambit of the qualified exemption created by section 24(1), with the result that section 24 could be rendered redundant. In those circumstances a true construction of the language the expression "relates to" must lead to the conclusion that it means "relate directly to", with the result that the



Information Commissioner was wrong to conclude that it could include an indirect connection, subject to a remoteness test.

38. The Information Commissioner, supported by the Home Office, argued that the expression must be construed broadly. Mr Knight drew our attention to a number of First-tier Tribunal cases in which this had been stated and suggested that, while they did not constitute binding authority, the consistency of approach demonstrated that there was no justification for limiting the scope of the exemption by importing the word “directly”.
39. In our view there is no justification for creating a connection between sections 23 and 24, which the Parliamentary Draftsman did not provide. The expression “relates to” is a broad term, whatever its context, and does not require to be qualified by the addition of “directly”. While not following earlier First-tier Tribunal decisions as precedent, we agree with the general approach adopted by them to a provision which was clearly intended to provide security bodies with extensive protection from disclosure. In our view the Information Commissioner was correct to base his decision on the broad principle that, to be exempt, the requested information would need to be “within the territory” of one of the security bodies.
40. The Information Commissioner was also right to concede, in both the Decision Notice and his skeleton argument on this appeal, that a test of remoteness should apply. On this point we reject the Appellant’s argument that the very application of a remoteness test to an absolute exemption (and the consequential need to conduct a factual investigation involving closed evidence) represented an error of law.
41. The Information Commissioner argued that the SPoC List was not too remote from, and did “relate to”, one or more security body. The Appellant argued, as an alternative to his primary argument on the point, that the names and ranks of people who may have liaised with a security body in the past, or may do so in the future, is, in the words of his skeleton argument “manifestly so remote as to fall outwith the sensible application of section 23(1)”.
42. The evidence of Mr Hirsch was relied on by the Information Commissioner to support his argument. It showed, the Information Commissioner argued, that SPoCs were inherently likely to be carrying out a role which requires more than occasional liaison with Security Bodies. A particular form of possible liaison was identified in closed evidence and is referred to in the confidential annex to this decision.

The evidence, he argued, demonstrated that a SPoC would have sufficiently close and regular contact with Security Bodies that disclosure of the identities of the SPoCs would be disclosure of matter which (quoting the First-tier Tribunal in *APPGER v Information Commissioner & Foreign and Commonwealth Office* [2012] 1 Info L R 258) “touches or stands in some relation to” such a body.

43. We think that, although the Information Commissioner correctly identified the test to be applied he fell into error in his Decision Notice in its application to the facts of this case. The SPoC list contains information about individuals performing a particular role within the RIPA regime. Their actions may lead, on occasions, to a Security Body becoming involved in the broad investigation of which the acquisition of Communications Data was a part. In those and other circumstances an individual SPoC may find himself or herself working in cooperation with the staff of a Security Body. While information about those activities would certainly be properly described as relating to the Security Body, the information about the identity and rank of SPoCs who may or may not become involved from time to time could not. It is simply too remote.

### Issue 3: SPoC list exempt under FOIA section 40(2)?

44. FOIA section 40(2) provides that information is exempt information if it constitutes personal data of a third party the disclosure of which would contravene any of the data protection principles.

45. Personal data is itself defined in section 1 of the Data Protection Act 1998 (“DPA”) which provides:

*“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”*

46. The data protection principles are set out in Part 1 of Schedule 1 to the DPA. The only one having application to the facts of this Appeal is the first data protection principle. It reads:

*“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 ...”*

Schedule 2 then sets out a number of conditions. The only relevant ones, for the purpose of this appeal, are the following:

*“1. The data subject has given his consent to the processing.”*

And

*“6.(1)The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.”*

The term “processing” has a wide meaning (DPA section 1(1)) and includes disclosure.

47. A broad concept of protecting, from unfair or unjustified disclosure, the individuals whose personal data has been requested is a thread that runs through the data protection principles, including the determination of what is “necessary” for the purpose of identifying a legitimate interest. In order to qualify as being “necessary” there must be a pressing social need for it - *Corporate Officer of the House of Commons v Information Commissioner and others* [2008] EWHC 1084 (Admin).

48. In determining whether or not disclosure of the names of SPoCs would be contrary to the data protection principles we have to consider:

- i. whether disclosure at the time of the information request would have been necessary for a relevant legitimate purpose; without resulting in
- ii. an unwarranted interference with the rights and freedoms or legitimate interests of individual SPoCs.

And if our conclusion on those points would lead to a direction that the information should be disclosed we have also to consider:

- iii. whether disclosure would nevertheless have been unfair or unlawful for any other reason.

49. In respect to the issue of fair and lawful processing under (iii) above we have to bear in mind guidance provided in paragraph 1(1) of Part II of Schedule 1 to the DPA, which provides:

*“In determining for the purposes of the [first data protection principle] whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.”*

50. The Appellant did not challenge that the requested information in this case did constitute the personal data of the individual SPoCs. However, he argued, first, that the individuals had effectively consented

to disclosure by accepting employment with a police force. Such forces, he argued, habitually make the name and rank of officers available to the public, including the indications incorporated on the uniforms of officers. We reject this argument because, as the evidence of the Home Office's witnesses disclosed, not all SPoCs are warranted officers (as opposed to civilians employed to undertake administrative work in support of such officers) and the disclosure of rank and number by uniformed officers does not disclose the fact that he or she is performing the role of a SPoC.

51. It was said by the Appellant, in support of his argument that a legitimate interest in disclosure existed for the purpose of condition 6(1), that this arose from the requirement to hold police forces to account for their activities under RIPA and the interest of investigative journalists to ensure that this happened. The Home Office argued that this fell well short of the "pressing social need" identified in the *Corporate Office of the House of Commons* case, particularly in light of the public scrutiny of the process which was already provided through the activities of the Interception of Communications Commissioner. The Home Office urged us to consider, in particular, whether the names of SPoCs would contribute anything to public scrutiny of, or debate in relation to, the operation of the RIPA regime. The Appellant addressed that point in very clear terms in his closing remarks during the hearing. He made it quite clear that he considered that individual accountability at all levels, including SPoCs, was an essential protection in light of the intrusive nature of RIPA procedures and the inadequacy, in his view, of the organisational and structural safeguards that had been put in place against the potential corrupt use of power.
52. We reject the Appellant's argument on the point. It seems to us that his arguments were more appropriately directed at a revision of the RIPA system, rather than the disclosure of the names of individuals. Public scrutiny might be facilitated by, for example, disclosure about the seniority of those performing the role of a SPoC, the training they undertook and the supervision to which they were subject. But the Appellant did not, in our view, make out a case that the disclosure of individual names would contribute to that process.
53. The Home Office argued that such legitimate interest in disclosure as existed carried little weight in comparison with the very considerable interference that SPoCs would suffer if their names were disclosed. The Appellant stressed the public nature of the work undertaken by SPoCs and the fact that some of them had self-publicised their role. The Home Office, by contrast, drew particular attention to the perceived danger of individual SPoCs being targeted by criminals with

a view to corrupting them and using them to undermine police activities. Although the Home Office evidence on this was criticised by the Appellant and challenged on cross examination, we accept that there would be a risk of SPoCs being targeted in the way suggested and that individuals performing the role of a SPoC are entitled to expect protection from attempts to corrupt them. We accept, too, that those fulfilling the role of SPoC are frequently relatively junior and not performing a public-facing role.

54. We conclude that there would be a justifiable expectation among SPoCs, as a group, that their individual identities would not be disclosed. We conclude, too, that the public interest in disclosure is light, for the reasons put forward in argument by the Home Office. The consequent need to avoid unwarranted interference with the individuals' right to privacy outweighs, comfortably, that very limited interest in disclosure. In our view, therefore, the exemption does apply to the names of SPoCs and the Home Office was entitled to refuse disclosure on that basis.

#### Issue 4: SPoC list exempt under FOIA section 31?

55. The relevant part of FOIA section 31 reads:

*“Information...is exempt information if its disclosure under this Act would, or would be likely to, prejudice-*  
*(a) the prevention or detection of crime.”*

56. The evidence of Mr Hirsch and Mr Higgins sought to highlight that there was a real risk that disclosure of the names of SPoCs would be likely to prejudice the prevention or detection of crime because it would make it easier and less risky for third persons to approach SPoCs and persuade them, by duress or corrupt offers, to undermine the security of the RIPA system for securing evidence. Even if the attempts to corrupt failed, it was said that individuals would be discouraged from accepting the role of SPoC, or remaining in post, if they thought such approaches were likely to occur. We have already commented on the likelihood of approaches being made, when reviewing the evidence in the context of the SPoC's right to privacy. We conclude that, contrary to the Appellant's argument that the Home Office's case on the point was “fanciful”, there is a level of risk of such unlawful approaches succeeding and of the fear of such approaches being made having the effect of discouraging individuals from seeking, or retaining, the role of a SPoC. Although we felt that some of the Home Office evidence

lacked specific information on attempts to corrupt SPoCs, whether successful or not, and that its own attempts to discourage self-publication were unconvincing, we nevertheless concluded that the risk was sufficiently strong to fall within the meaning of the phrase “likely to prejudice”, with the result that the exemption is engaged.

57. As FOIA section 31 is a qualified exemption we must consider, too, whether the public interest in maintaining the exemption outweighs the public interest in disclosure (FOIA section 2(2)(b)). We are satisfied that, for the reasons given earlier, there is very little public interest in having the names disclosed and the risk of prejudice in our view clearly outweighs it. The Home Office was therefore, again, entitled to refuse disclosure on the basis of FOIA section 31.

Issue 5: SPoC list exempt under FOIA section 38?

58. The relevant part of FOIA section 38 reads:

*“Information is exempt information if its disclosure under this Act would, or would be likely to-*

- (a) endanger the physical or mental health of any individual, or*
- (b) endanger the safety of any individual”*

59. The Home Office relied upon the same evidence as referred to above in support of its claim that the exemption applied and the Appellant again asserted that the perceived risks were fanciful, a contention supported in part by an argument, which we do not accept, arising from a perceived illogicality in the drafting of sections 31 and 38 when read together.

60. We have previously explained why we accept that there is a risk of SPoC’s being approached by criminals or others intent on undermining the effectiveness of the RIPA regime. The evidence that the approach may be accompanied by actual or threatened violence, or that a refusal to co-operate may result in violence, was less well supported by evidence. We felt that the witnesses engaged in a degree of speculation in this part of their evidence. The conclusion they feared, however, is one that would flow logically from initiating communications designed to corrupt the relevant official. It is therefore justifiable to regard it as a result that would be likely to flow from the disclosure of names and to conclude that the exemption is engaged.

61. The public interest in maintaining the exemption would again outweigh the public interest in disclosure, given the very limited public interest in

disclosure and the risk, at the level we have identified, of physical harm coming to individual SPoCs.

### Conclusion

62. We conclude that the Home Office was entitled to refuse disclosure on the basis that the requested information was exempt under FOIA sections 40, 31 and 38 and that, in the case of the latter two, the public interest in maintaining the exemption outweighed the public interest in disclosure. The Decision Notice was therefore correct in its conclusion, although we reach the same conclusion by a different route.

63. Our decision is unanimous.

**Chris Ryan**  
Judge

6 May 2014