

# Decision Notice

---

**Decision 195/2016: Mr Alastair Tibbitt and Community Safety Glasgow**

---

## **CCTV information**

Reference No: 201501718

Decision Date: 15 September 2016



Scottish Information  
Commissioner

## Summary

---

On 9 June 2015, Mr Tibbitt asked Community Safety Glasgow (CSG) for information about its CCTV processes and operations.

CSG confirmed that it held some of the information he requested. It disclosed some information, and withheld the remainder under FOISA exemptions. Following a review, Mr Tibbitt remained dissatisfied and applied to the Commissioner for a decision.

The Commissioner investigated and found that some of the information CSG had withheld should have been disclosed. She ordered CSG to disclose the information to Mr Tibbitt.

The Commissioner also found that CSG had failed to give Mr Tibbitt notice that it did not hold all the information he requested and failed to conduct adequate searches for that information when responding to Mr Tibbitt. She required CSG to disclose further information to Mr Tibbitt.

## Relevant statutory provisions

---

Freedom of Information (Scotland) Act 2002 (FOISA) sections 1(1), (4) and (6) (General entitlement); 2(1)(b) (Effect of exemptions); 17(1) (Notice that information is not held); 30(c) (Prejudice to effective conduct of public affairs); 35(1)(a) and (b) (Law enforcement)

The full text of each of the statutory provisions cited above is reproduced in Appendix 1 to this decision. Both Appendices form part of this decision.

## Background

---

1. On 9 June 2015, Mr Tibbitt made a nine-part request for information to CSG, which included the following:
  - Part 2: A copy of the current CSG CCTV Local Operations Manual in electronic format.
  - Part 8: Confirmation of the number of times the GSG CCTV system has been operated partially, or fully, by a third party organisation in the last three years. For each occurrence, if any, which third party agency took over control (or partial control) of the system, when control was given, and for how long.

The full text of Mr Tibbitt's request is reproduced in Appendix 2 to this decision. The Appendix forms part of the decision.

2. CSG responded on 6 July 2015. It informed Mr Tibbitt that it held some of the information he had requested. It disclosed some of that information, withholding the remainder under FOISA exemptions. For parts 2 and 8, CSG withheld the information under section 35 of FOISA, considering disclosure would, or would likely to, have a substantially prejudicial effect on a wide range of different law enforcement functions and activities.
3. On 6 July 2015, Mr Tibbitt wrote to CSG, requesting a review of its decision on the basis that he did not agree the exemptions applied. He believed it was important that CCTV equipment was used in a transparent manner if the public was to retain trust in the service.
4. CSG notified Mr Tibbitt of the outcome of its review on 4 August 2015.

5. For part 2, CSG upheld its original decision to apply section 35(1) fully. It considered disclosure of the information would be likely to prejudice substantially the prevention and detection of crime. It believed the public interest lay in relevant organisations being able to ensure crimes were prevented or detected and offenders apprehended or prosecuted, to ensure public safety.
6. For part 8, CSG upheld its original decision with modification. It informed Mr Tibbitt that Police Scotland had partially operated the CSG CCTV system on 483 occasions over the preceding three financial years. CSG upheld its decision to apply section 35(1) to the further breakdown elements requested. As with part 2, CSG believed the public interest favoured withholding the information.
7. On 18 September 2015, Mr Tibbitt wrote to the Commissioner, applying for a decision in terms of section 47(1) of FOISA. Mr Tibbitt stated he was dissatisfied with the outcome of CSG's review because he believed CSG had wrongly applied section 35(1) to parts 2 and 8 of his request, and that it had incorrectly assessed the public interest in understanding how public space CCTV was operated in Glasgow.

## **Investigation**

---

8. The application was accepted as valid. The Commissioner confirmed that Mr Tibbitt made a request for information to a Scottish public authority and asked the authority to review its response to that request before applying to her for a decision.
9. The case was allocated to an investigating officer and, on 18 November 2015, CSG was notified in writing that Mr Tibbitt had made a valid application. CSG was asked to send the Commissioner the information withheld from Mr Tibbitt and this was provided by CSG.
10. Section 49(3)(a) of FOISA requires the Commissioner to give public authorities an opportunity to provide comments on an application. CSG was invited to comment on this application and answer specific questions, with particular reference to (i) the searches carried out to identify the information falling within scope and (ii) its application of section 35(1) to withhold the information requested.
11. CSG provided submissions to the investigating officer. Clarification of aspects of these was sought, and obtained, during the investigation.
12. As CSG was withholding information under an exemption in FOISA which is subject to the public interest test, Mr Tibbitt was invited to provide submissions on why he believed it was in the public interest for the information to be disclosed. Mr Tibbitt provided submissions, focused on part 2 of his request. He also confirmed that he was content with the redaction of personal data and direct dial telephone numbers.

## **Commissioner's analysis and findings**

---

13. In coming to a decision on this matter, the Commissioner has considered all of the withheld information and the relevant submissions, or parts of submissions, made to her by both Mr Tibbitt and CSG. She is satisfied that no matter of relevance has been overlooked.

## Information held

14. CSG was asked to provide an explanation of the searches it had undertaken to identify, locate and retrieve the requested information. This was so that the Commissioner could form a view about whether CSG had identified and located all relevant information it held falling within the scope of the request.

### *Part 2 – Local Operations Manual*

15. CSG explained that the request had been passed to the Glasgow Operations Centre (GOC) Operations Manager to identify and locate the relevant document. CSG submitted that no other searches were considered to be necessary as the relevant document was identified and located.
16. Having considered CSG's submissions, the terms of the request and the withheld information, the Commissioner is satisfied that the searches undertaken by CSG were adequate, in the circumstances, to identify the information relevant to this part of Mr Tibbitt's request.

### *Part 8 – Third party operation of CCTV system*

17. CSG explained that the request had been passed to the GOC Operations Manager to identify and locate any information held and which fell within the scope of this part of Mr Tibbitt's request. CSG considered this individual to be best placed to identify the relevant information as the Operations Manager was fully aware of the audit and security requirements of the GOC.
18. CSG explained that CCTV operations had been relocated on a phased basis from Blochairn to GOC in January 2014, following which there had been changes to the procedures and authorisation process. CSG described the processes before and after the relocation, including details of the documentation that required to be completed.
19. The GOC Operations Manager had identified the following as containing relevant information falling within the scope of the request:
  - (i) Directed Surveillance Authority (DSA) forms from within the relevant period
  - (ii) excerpt of the electronic database for the relevant period
  - (iii) visitors log for the relevant period.
20. CSG submitted that the information identified did not contain answers to some of Mr Tibbitt's questions.
21. At the time of relocation, CSG explained, all DSA forms and associated visitors log books for the period prior to relocation were destroyed. In accordance with section 17 of FOISA, therefore, CSG submitted that it did not hold any information for part 8 of Mr Tibbitt's request, relating to the period prior to January 2014.
22. In relation to the first part of part 8 (the "number of times" the system had been operated by a third party), CSG informed the Commissioner that the figure disclosed to Mr Tibbitt at review stage was incorrect. It provided the Commissioner with a revised figure for the number of times Police Scotland had made partial use of the CCTV system (in the period following relocation). CSG apologised for this, explaining it was due to human error.
23. For the period following relocation, CSG submitted that the information it held relating to "when" and "how long" control was given was not held in a format that could be disclosed. It

explained that to answer these parts of the request, new data would need to be created through manipulation of the existing datasets. CSG informed the Commissioner that, as it considered this information to be exempt from disclosure in terms of section 35(1)(a) and (b) of FOISA, it had not carried out this exercise as to do so would require a significant investment in staff time, resulting in diversion of resources away from core service delivery.

24. CSG was also of the view that complying with Mr Tibbitt's request for information on "when" and "how long" control was given would exceed the upper cost limit of £600 allowed by section 12(1) of FOISA. It explained that all three elements of the information identified in paragraph 19 above would need rearranging so the data could be manipulated in order to provide the answers. This would involve collating DSA forms, for example, by either operation or date, and cross-referencing them with the information held in the electronic matrix and visitors log. Thereafter, a new document would have to be created with manual input of the date, time and duration for each occasion when control had been given. This process would need to be repeated for each DSA form held for the period of the request (i.e. that following relocation). CSG provided details of its calculations and a sampling exercise.
25. Having examined the withheld information provided by CSG for part 8 of Mr Tibbitt's request, together with CSG's submissions on the information held falling within scope, it was clear to the investigating officer that there were discrepancies. CSG was asked to clarify a number of points regarding the information it held for this part of the request so that a view could be formed about whether a full or partial data set was held that could answer this part of the request, or elements of it. CSG was also asked to provide full submissions relating to its reliance on section 12(1) of FOISA, for the elements of the request relating to "when" and "how long" control was given.
26. CSG provided further submissions explaining in more detail the extent of the information held for this element of Mr Tibbitt's request. It confirmed that the time period now being considered was the three year period immediately prior to the date of the request, i.e. from 10 June 2012 to 9 June 2015.
27. To the extent that information was held, CSG submitted that the details requested by Mr Tibbitt could be extracted.
28. CSG informed the Commissioner that it was no longer relying on section 12(1) in relation to this element of the request. In respect of the information that could be extracted, CSG confirmed it wished to withhold that information in terms of section 35(1)(a) and (b) and section 30(c) of FOISA.
29. After considering CSG's further submissions, additional issues arose requiring clarification: specifically in relation to the number of DSA forms held, and information held relating to "when" control was given. CSG was again asked to provide further submissions clarifying a number of points regarding the information it held for this part of Mr Tibbitt's request.
30. CSG explained there had been a misunderstanding with the data originally provided, and provided revised submissions explaining fully the extent of the information held for this part of the request, showing how that data had been identified. It apologised for any confusion caused.
31. CSG reaffirmed that all hard copy paperwork relating to DSA visits for the period prior to relocation had been confidentially disposed of in January 2014. However, as a result of a misunderstanding within CSG, it had become apparent that the overall figure for the number of DSA visits had not been derived from hard copy paperwork, as originally submitted, but

from electronically held KPI data that dated back to January 2013 (i.e. prior to the date of relocation). CSG explained that this data, which logged the number of DSA visits per month, was collected for internal reporting purposes and had been used to produce the overall number of DSA visits. CSG provided the Commissioner with the KPI data.

32. With regard to the number of visits, CSG explained that it had erroneously assumed that the revised figure provided in its earlier submissions related to the three year period immediately preceding the request. CSG submitted that it had since been ascertained that this figure actually related to the three financial years 1 April 2012 to 31 March 2015. It further explained that this figure did not include any visits up to 31 December 2012, given that the recording of KPI statistics only came into effect in January 2013.
33. Due to an error in extracting the monthly KPI data, CSG confirmed that the revised figure provided in its earlier submissions was incorrect. A further discrepancy was identified when these data were cross-referenced with the hard copy DSA forms. CSG was unable to determine whether this was due to an error in capturing the KPI data, or whether the KPI data was correct and there were some visits for which no DSA form existed.
34. To summarise, for the period covering this part of Mr Tibbitt's request (i.e. 10 June 2012 to 9 June 2015), CSG confirmed that it held no information for the period 10 June 2012 to 31 December 2012, for which there were neither DSA forms nor KPI records.
35. For the period 1 January 2013 to 9 June 2015, CSG confirmed that it held information and provided the Commissioner with a new, revised figure for the "number of times" the system had been operated by a third party. This comprised:
  - (i) the number of initial visits only (for each operation) for the period 1 January 2013 to 31 March 2014; and
  - (ii) the number of initial and subsequent visits (for each operation) for the period 1 April 2014 to 9 June 2015.
36. In respect of the dates of visits, CSG explained that it held the dates of initial visits only for the period 1 January 2014 to 31 March 2014, and the dates of initial and subsequent visits for the period 1 April 2014 to 9 June 2015.
37. Regarding "how long" the system had been operated by a third party, CSG explained that the DSA forms had included a field for the arrival time from March 2014, which had been completed in the majority of cases. They did not record departure time, however, so it held no information from which durations of visits could be calculated.

#### Part 8 – Commissioner's conclusions on information held

38. Under section 1(4) of FOISA, the information to be provided in response to a request under section 1(1) is that falling within the scope of the request and held by the authority at the time the request is received.
39. The standard of proof to determine whether a Scottish public authority holds information is the civil standard of the balance of probabilities. In determining where the balance of probabilities lies, the Commissioner considers the scope, quality, thoroughness and results of the searches carried out by the public authority. She also considers, where appropriate, any reason offered by the public authority to explain why it does not hold the information.
40. Having considered all the relevant submissions and the terms of the request, the Commissioner is satisfied that, by the end of the investigation, CSG had taken adequate,

proportionate steps to establish the extent of information held that was relevant to the request.

41. The Commissioner accepts CSG's final position on what it did and did not hold. She is satisfied that CSG did not hold all of the information falling within the scope of part 8 of Mr Tibbitt's request: it held information for the "number of times" from 1 January 2013 to 9 June 2015, and the dates of visits from 1 January 2014 to 9 June 2015.
42. The Commissioner is concerned that it took a number of attempts during the investigation for CSG to clarify what it did and did not hold in relation to part 8 of the request. This was something it should have addressed when responding to Mr Tibbitt's request or, at the latest, his requirement for review. Given that it was not resolved definitively until during the investigation, it is clear that CSG failed to take adequate steps to identify and locate all the relevant information when responding to Mr Tibbitt. In this respect, the Commissioner finds that CSG failed to comply with section 1(1) of FOISA.
43. Not only was this a breach of FOISA, it resulted in avoidable delay for the applicant and avoidable expense to the public purse. The Commissioner strongly urges the CSG to reflect on its FOI practice with a view to avoiding similar situations in the future so that applicants receive the information they request, or an explanation as to why it is being withheld, at the earliest opportunity.

#### **Section 17(1) of FOISA – Notice that information is not held**

44. Under section 17(1) of FOISA, where an authority receives a request for information it does not hold, it must give the applicant notice in writing to that effect. In this case, CSG did not provide Mr Tibbitt with such a notice in respect of any element of part 8 of his request.
45. Given that CSG did not hold all elements of the information requested, it had a duty to issue a notice in writing to that effect, to comply with the terms of section 17(1) of FOISA.
46. As CSG failed to provide such a notice to Mr Tibbitt, the Commissioner finds that it failed to comply with the requirements of section 17(1) of FOISA.

#### **Sections 35(1)(a) and (b) of FOISA – Law enforcement**

47. CSG applied the exemptions in section 35(1)(a) and (b) of FOISA to parts 2 and 8 of Mr Tibbitt's request.
48. Section 35(1)(a) exempts information if its disclosure would, or would be likely to, prejudice substantially the prevention or detection of crime. As the Commissioner's guidance<sup>1</sup> on this exemption highlights, the term "prevention or detection of crime" is wide ranging. It encompasses actions taken to anticipate and prevent crime, or to establish the identity and secure prosecution of people suspected of being responsible for committing a crime. This could mean activities in relation to specific (anticipated) crime or wider strategies for crime reduction and detection.
49. Section 35(1)(b) exempts information if its disclosure would, or would be likely to, prejudice substantially the apprehension or prosecution of offenders. As the Commissioner's guidance also states, there is likely to be an overlap between information relating to "the apprehension or prosecution of offenders" and that relating to "the prevention or detection of crime". Section 35(1)(b) is narrower and focusses on the process of identifying, arresting or

---

<sup>1</sup> <http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/section35/Section35.asp>

prosecuting those suspected of being responsible for unlawful activity. Again, this term could refer to the apprehension or prosecution of specific offenders or to more general techniques such as investigative processes used, information received, or guidance given, and strategies designed for these purposes.

50. There is no definition of "substantial prejudice" in FOISA, but the Commissioner's view is that authorities have to be able to identify harm of real and demonstrable significance. The harm would also have to be at least likely, and more than simply a remote possibility.
51. The exemptions in section 35(1) are subject to the public interest test in section 2(1)(b) of FOISA.

#### *Part 2 – Local Operations Manual*

52. During the investigation, CSG informed the Commissioner that it had reconsidered its position and was prepared to disclose some of the information in the Manual to Mr Tibbitt. CSG disclosed a redacted version of the Local Operations Manual to Mr Tibbitt on 19 February 2016.
53. CSG confirmed it wished to maintain reliance on section 35(1)(a) and (b) of FOISA to withhold the redacted information.
54. In its submissions to the Commissioner, CSG maintained that there would be substantial prejudice to the prevention and detection of crime (section 35(1)(a) of FOISA), and the apprehension and prosecution of offenders (section 35(1)(b) of FOISA), if the redacted information were to be disclosed. This was because it would disclose:
  - (i) operational information on a restricted and secure environment;
  - (ii) information which could prejudice ongoing or related investigations: taken with other information already in the public domain, it would identify potential consequences of DSA activities which might disclose future operations;
  - (iii) sensitive information on systems and system capabilities, which could allow counter-measures to be taken to avoid detection;
  - (iv) information on scope and location that would have a detrimental impact on the personal safety of officers;
  - (v) operational information which could allow individuals to implement counter-measures;
  - (vi) confidential information relating to disaster recovery location and operations, which could allow potential for disruption of the same; and
  - (vii) information on third party partner systems, intelligence and operations based in the GOC.
55. CSG submitted that the apprehension and prosecution of offenders would be further substantially prejudiced as:
  - (i) disclosure of restricted operational information into the public domain would provide increased awareness of CCTV operations in Glasgow, including their limitations, to those involved in serious and organised crime; and
  - (ii) disclosure would have the potential to cause a displacement of crime and anti-social behaviour to locations with no CCTV coverage.

56. During the investigation, CSG was asked to consider whether it would be prepared to disclose to Mr Tibbitt any further information in the Manual.
57. CSG informed the Commissioner that, having considered its position, it remained concerned about the substantial prejudice to the prevention of crime and the apprehension of offenders, should any further information be disclosed. In particular, CSG identified specific information which, in its view, could increase the possibility of a successful security breach, raising concerns regarding staff safety and the operation of the GOC.
58. Disclosure of the full Manual, CSG submitted, would reveal information on every aspect of the service's operations, including the procedures and protocols in place for building security, systems usage and security, fire evacuation plans and procedures, procedures for access to the GOC and CCTV footage. CSG considered disclosure of this information might undermine the security of the Centre and the safety of staff.
59. CSG contended that, to mitigate against hostile reconnaissance it was necessary to restrict the level and type of information disclosed into the public domain, such as asset locations, asset access and operational information. It believed that such information might assist individuals intent on such actions to access systems, or identify areas as possible targets.
60. CSG argued that as the Manual was an internal and restricted document for key staff only, full disclosure could have serious implications for the running of the public space CCTV network nationally. It believed disclosure posed a risk to safeguarding staff security, the physical environment, and day-to-day activities in the city.

Part 2 – Commissioner's conclusions whether sections 35(1)(a) and (b) apply

61. The Commissioner must consider whether disclosure would, or would be likely to, cause substantial prejudice to the prevention or detection of crime (section 35(1)(a)) or the apprehension or prosecution of offenders (section 35(1)(b)).
62. The Commissioner has considered CSG's submissions on this point, along with full examination of the withheld information. She is not persuaded that the submissions adequately explain how disclosure of the majority of the withheld information would have the effect claimed.
63. The Commissioner agrees with CSG that disclosure of information about specific investigative processes, locations, resources and disaster recovery procedures would have an adverse impact upon security and the effective operation of the Centre. It would also have the potential, in the wrong hands, to enable disruption to agreed procedures in the event of disaster recovery. Consequently, she is satisfied that disclosure of this information would, or would be likely to, prejudice substantially both the prevention or detection of crime and the apprehension or prosecution of offenders, and so is exempt from disclosure under the exemptions in section 35(1)(a) and (b) of FOISA.
64. The Commissioner considers that the remainder of the withheld information is general and factual information that any reasonable person would expect to be included in such a manual. It contains nothing so obviously operationally sensitive that, in the Commissioner's view, disclosure would, or would be likely to, cause the prejudice argued by CSG.
65. The Commissioner is not persuaded by CSG's arguments that the level of detail is such that criminals would be able to use this information to access systems, or identify areas as possible targets. Nor that they would be likely to tailor their activities to particular areas in

the remote chance that there would be less possibility of their activities being captured on CCTV.

66. In conclusion, the Commissioner accepts the arguments put forward by CSG for withholding information concerning specific investigative processes, locations, resource levels and disaster recovery procedures under section 35(1)(a) and (b) of FOISA, but she is not satisfied that disclosure of the remainder of the information in the Manual would, or would be likely to, prejudice substantially CSG's or Police Scotland's ability to prevent or detect crime or apprehend or prosecute offenders.
67. As the Commissioner is not satisfied that the remaining information was correctly withheld under section 35(1)(a) and (b) of FOISA, she is not required to go on to consider the application of the public interest test in section 2(1)(b) to it.
68. As no other exemption has been claimed to justify the remaining information being withheld, the Commissioner requires CSG to disclose it to Mr Tibbitt, subject to the redaction of personal data and direct dial or internal telephone numbers (which Mr Tibbitt has confirmed he does not require). The information to be disclosed will be indicated on a copy of the Manual accompanying the decision to CSG.
69. As the exemptions have been found to apply to the withheld information concerning specific investigative processes, locations, resource levels and disaster recovery procedures, the Commissioner is now required (for this information) to go on to consider the public interest test in section 2(1)(b) of FOISA.

## Part 2 - Public Interest Test

70. The exemptions in section 35(1)(a) and (b) are both qualified exemptions, which means their application is subject to the public interest test set out in section 2(1)(b) of FOISA. The Commissioner must go on to consider whether, in all the circumstances of the case, the public interest in disclosing the withheld information (insofar as she has found it to be exempt) is outweighed by the public interest in maintaining the exemptions in section 35(1)(a) and (b) of FOISA.
71. CSG acknowledged that there was a public interest in openness and transparency surrounding how a public-facing CCTV system is operated.
72. CSG submitted that the Code of Practice for Public Space CCTV, a public document outlining the key aspects of the operations and workings of the service, went some way to addressing the public interest in understanding the operation of public space CCTV without compromising its effective use.
73. CSG contended there was a significant public interest in safeguarding the security and effective operation of the GOC, and the use of its public space CCTV system by Police Scotland, CSG and the Council. This was vital in ensuring public safety and reassurance, the effective prevention and detection of crime and the apprehension and prosecution of offenders. CSG believed disclosing the withheld information would prejudice this purpose. It considered there to be no public interest in the disclosure of information that would allow individuals to understand the limitations of the system, thereby allowing counter-measures to be taken to circumvent the prevention and detection of crime and the apprehension and prosecution of offenders.
74. CSG believed that, on balance, the public interest in ensuring Police Scotland's ability to carry out its role in preventing and detecting crime, and apprehending and prosecuting

offenders, outweighed the public interest in openness and transparency, which (in its view) was met by the disclosure of the redacted Manual in any case. It maintained that the redacted Manual provided sufficient background understanding of how CSG operated its public space CCTV, without prejudicing substantially the prevention and detection of crime and the apprehension and prosecution of offenders.

75. Mr Tibbitt submitted that the Manual had a specific purpose set out by the Scottish Ministers<sup>2</sup>. He referred to:
- (i) concerns raised by civil liberties groups and MSPs, alleging that neither Police Scotland nor CSG had provided clear guidance to camera operators taking account of those rules;
  - (ii) the Westminster Government's plans to introduce new legislation on this subject; and
  - (iii) wider national security concerns relating to counter-terrorism.
76. In this context, Mr Tibbitt believed it was vital that public authorities were transparent about the current management practices used when managing public space CCTV.
77. Mr Tibbitt believed the public interest lay in being able to determine whether the document complied with national guidance and other statutory rules, including that concerning data protection and surveillance.
78. Mr Tibbitt informed the Commissioner he would be happy to receive a copy of the Manual, with the redaction of any information, where necessary, that would compromise national security or law enforcement activities. He further confirmed that he would be happy for any personal data or telephone numbers to be redacted from any information deemed suitable for disclosure under FOISA.

#### Part 2 - Commissioner's conclusions on public interest test

79. The Commissioner acknowledges the general public interest in transparency and accountability. She accepts that disclosure of the information would allow public scrutiny and assessment of the procedures followed by CSG in relation to the operation of its public space CCTV system. This, in turn, would contribute to reassuring the public about the extent to which CSG was managing its public space CCTV in line with the requirements set out by the Ministers. To a large degree this will be met by disclosure of the information the Commissioner has found not to be exempt, together with the information already disclosed by CSG.
80. On the other hand, the Commissioner accepts that there is a significant public interest in CSG ensuring that any risks to the security and operation of the GOC and the CCTV system are managed and mitigated.
81. The Commissioner has already acknowledged that disclosure of the information would, or would be likely to, lead to substantial prejudice for the purposes of section 35(1)(a) and (b) of FOISA. In this regard, she considers there is no public interest in the disclosure of information which could prejudice substantially the effectiveness and security of the system, its effective operation and the Centre itself, as this would have a direct impact on CSG's and Police Scotland's ability to prevent and detect crime, and apprehend and prosecute offenders.

---

<sup>2</sup> <http://www.gov.scot/Publications/2011/03/18085554/2>

82. Having balanced the public interest arguments for and against disclosure, the Commissioner is satisfied that, in all the circumstances of the case, the public interest arguments in maintaining the exemptions in section 35(1)(a) and (b) outweigh those in disclosure of the information under consideration.
83. The Commissioner therefore finds that CSG was entitled to withhold the remaining withheld information (concerning specific investigative procedures, locations, resource levels and disaster recovery procedures) under the exemptions in section 35(1)(a) and (b) of FOISA.

*Part 8 – Third party operation of CCTV system*

84. Having established the extent of the information held by CSG falling within the scope of part 8 of Mr Tibbitt's request, CSG informed the Commissioner that it wished to withhold this information under section 35(1)(a) and (b) of FOISA.
85. CSG argued that disclosure of this information would jeopardise Police Scotland operations. It submitted that raising awareness of specific instances when Police Scotland have used public space CCTV as part of covert surveillance operations might inform individuals intent on criminal activity of ongoing and previous operations and impact adversely on the effectiveness of using this method of detecting crime and prosecuting offenders. CSG argued that this could, consequently, represent an increased danger to the public should this method of detection and prosecution become less effective as a result of disclosure. It believed knowledge of arrests or police intervention, combined with this information, could alert those involved in serious or organised crime to instances in which the police had operated undercover within their organisations.
86. CSG submitted that disclosure of the information would jeopardise current or future Police Scotland surveillance operations into serious and organised crime, by providing criminals with information on times, locations and dates of operations. It considered disclosure would also reveal information on possible Police Scotland operations and tactics.
87. CSG further submitted that disclosure of the information would have implications for the protection of sources. It contended that operational details, times and dates could be linked back to possible source information provision, which could have severe consequences for police intelligence operations.
88. CSG argued that disclosing core elements of information relating to previous or ongoing police operations might jeopardise the role played by public space CCTV in tackling and preventing serious crime and anti-social behaviour, and making communities safer and crime-free.
89. CSG continued that disclosure of such a detailed level of information might compromise the role played by public space CCTV in supporting Police Scotland's ability to prevent, detect and deter crime. Added to information in the public domain, and the existing knowledge of criminals, CSG believed this information would allow such individuals to assess police intelligence on previous and ongoing serious and organised crime activities. Providing information on dates and duration might enable the analysis of usage and possible locations where public space CCTV had been utilised to support Police Scotland in tackling serious and organised crime.

Part 8 – Commissioner's conclusions on whether sections 35(1)(a) and (b) apply

90. The Commissioner must consider whether disclosure would (or would be likely to) cause substantial prejudice to the prevention or detection of crime (section 35(1)(a)) or to the

apprehension or prosecution of offenders (section 35(1)(b)). She must do this on the basis of the submissions she has received (or those parts of them she considers relevant), and their application at the time CSG responded to Mr Tibbitt's requirement for review.

91. The Commissioner acknowledges that information about dates, times, durations and locations of police operations, where CCTV surveillance has been deployed by the police could, when taken together with information already known to criminals, allow those involved in serious and organised crime to make a more informed guess as to the level of police surveillance, tactics and activities in an area, during the period stated.
92. She also recognises the possibility that such level of detail, taken as a whole, might present an increased risk to source information provision, which would impact adversely on intelligence-led police operations.
93. The Commissioner notes that Mr Tibbitt has not requested details about locations where CCTV surveillance has been carried out by third-party users of the system and that CSG holds no information relating to specific times and duration of usage. This leaves only the information about the corresponding dates which, as has already been ascertained, is held only in part.
94. The Commissioner appreciates the importance of Police Scotland's role in relation to the prevention and detection of crime and the apprehension and prosecution of offenders. She also appreciates that they need to be able to carry out this function in an intelligence-led manner, using effective methods and tactics. The Commissioner recognises the important role CCTV surveillance plays but notes that public space CCTV is not the only method of surveillance used by Police Scotland when developing intelligence about crime.
95. The Commissioner is not persuaded by CSG's submissions that disclosure of historical dates, in isolation from any other associated information, would result in the harm it identified.
96. For the reasons set out above, the Commissioner does not accept that disclosure of the withheld information (i.e. the dates) to Mr Tibbitt (and thereby into the public domain) would have caused, or would have been likely to cause, substantial prejudice to Police Scotland's ability to prevent or detect crime or apprehend or prosecute offenders. She does not believe such a conclusion can be reached on the basis of the arguments provided.
97. The Commissioner does not, therefore, accept that the exemptions in section 35(1)(a) and (b) of FOISA should be upheld in respect of the dates.
98. Given that the Commissioner does not accept the application of the exemptions, she is not required to consider the public interest test in section 2(1)(b) of FOISA.
99. CSG has also relied on section 30(c) of FOISA for the information identified for part 8 of Mr Tibbitt's request, so the Commissioner will now go on to consider its application of this exemption.

### **Section 30(c) of FOISA – Prejudice to the effective conduct of public affairs**

100. Section 30(c) of FOISA exempts information if its disclosure "would otherwise prejudice substantially, or be likely to prejudice substantially, the effective conduct of public affairs". The use of the word "otherwise" distinguishes the harm required from that envisaged by the exemptions in section 30(a) and (b). This is a broad exemption and the Commissioner expects any public authority citing it to show what specific harm would (or would be likely to)

be caused to the conduct of public affairs by disclosure of the information, and how that harm would be expected to follow from such disclosure.

101. Section 30(c) applies where the harm caused, or likely to be caused, by disclosure is at the level of substantial prejudice. There is no definition in FOISA of what is deemed to be substantial prejudice, but the Commissioner considers the harm in question must be of real and demonstrable significance. The authority must be able to satisfy the Commissioner that the harm would, or would be likely to, occur and therefore needs to establish a real risk or likelihood of actual harm occurring as a consequence of disclosure at some point in the near (certainly foreseeable) future, not simply that the harm is a remote possibility.
102. It is important for public authorities to treat each request for information on a case-by-case basis. Disclosure of information in one case should not be taken to imply that information of a particular type will routinely be disclosed in future. The circumstances of each case, including the content of the information under consideration and the timing of the request, must be taken into consideration.
103. CSG stated that DSA operations that had taken place in the last three years could be re-activated by Police Scotland, so the disclosure of dates, times and durations of such activities could prejudice future operations.

#### Part 8 – Commissioner’s conclusions on whether section 30(c) applies

104. Having fully considered CSG’s submissions on this point, as with section 35(1)(a) and (b), the Commissioner is not persuaded that the disclosure of historical dates in isolation, with no associated information, such as location or description of the operation, would cause the harm envisaged by CSG.
105. The Commissioner notes, from CSG’s submissions, that surveillance operations that have taken place in the last three years can be re-activated by Police Scotland. However, she is not persuaded that an individual, in the absence of any associated information describing the nature or location of that operation, would be able to connect only a date with any particular operation.
106. It has not been made evident to the Commissioner that there would be a direct link between a particular date and any operation that may be re-activated by Police Scotland at a later date, bearing in mind that information surrounding the details of any future re-activation is unlikely to be made public pro-actively.
107. In the absence of any remotely substantial explanation of the link, the Commissioner does not accept that disclosure of the withheld information (i.e. the dates) would, or would be likely to, prejudice substantially the effective conduct of public affairs. She does not believe such a conclusion can be reached on the basis of the arguments provided.
108. The Commissioner does not, therefore, accept that the exemption in section 30(c) of FOISA should be upheld in respect of the dates.
109. In conclusion, the Commissioner is not persuaded by CSG’s submissions that the exemption in section 30(c) of FOISA was correctly applied to the information it held and identified as falling within the scope of part 8 of Mr Tibbitt’s request (i.e. the dates).
110. Given that the Commissioner does not accept the application of the exemption, she is not required to consider the public interest test in section 2(1)(b) of FOISA.

## Compliance required

---

### **Part 2 of request – Local Operations Manual**

111. CSG is required to disclose to Mr Tibbitt the information in the GOC Operations Manual, subject to the redaction of:

- (i) any personal data and direct dial or internal telephone numbers, and
- (ii) information relating to specific investigative processes, locations, resource levels and disaster recovery procedures,

all of which will be marked on a copy of the Manual provided to CSG.

### **Part 8 of request – Information on third party operation of CCTV system**

112. CSG is required to provide Mr Tibbitt with information detailing the correct number of DSA visits for each of the periods 1 January 2013 to 31 March 2014 and 1 April 2014 to 9 June 2015.

113. CSG is required to disclose to Mr Tibbitt the dates when Police Scotland used the CCTV system during each of the periods 1 January 2014 to 31 March 2014 and 1 April 2014 to 9 June 2015.

## Decision

---

The Commissioner finds that Community Safety Glasgow (CSG) partially complied with Part 1 of the Freedom of Information (Scotland) Act 2002 (FOISA) in responding to the information request made by Mr Tibbitt.

The Commissioner finds that CSG complied with Part 1 of FOISA by correctly withholding some information under section 35(1)(a) and (b) of FOISA.

The Commissioner also finds that CSG failed to comply with Part 1 of FOISA by:

- (i) failing to take adequate steps to identify and locate all of the information requested by Mr Tibbitt. This was a failure to comply with section 1(1).
- (ii) failing to give notice, as required by section 17(1) of FOISA, that it did not hold all the elements of the information covered by part 8 of Mr Tibbitt's request.
- (iii) incorrectly withholding information under sections 35(1)(a), 35(1)(b) and 30(c) of FOISA. This was also a failure to comply with section 1(1).

The Commissioner therefore requires CSG to provide Mr Tibbitt with:

- (i) information from the GOC Operations Manual (subject to redaction as described in paragraph 111 above);
- (ii) the number of times Police Scotland used the CCTV system during each of the periods 1 January 2013 to 31 March 2014 and 1 April 2014 to 9 June 2015; and
- (iii) the dates corresponding to each of the occasions where Police Scotland used the CCTV system during each of the periods 1 January 2014 to 31 March 2014 and 1 April 2014 to 9 June 2015,

by **31 October 2016**.

## Appeal

---

Should either Mr Tibbitt or Community Safety Glasgow wish to appeal against this decision, they have the right to appeal to the Court of Session on a point of law only. Any such appeal must be made within 42 days after the date of intimation of this decision.

## Enforcement

---

If Community Safety Glasgow (CSG) fails to comply with this decision, the Commissioner has the right to certify to the Court of Session that CSG has failed to comply. The Court has the right to inquire into the matter and may deal with CSG as if it had committed a contempt of court.

**Rosemary Agnew**  
**Scottish Information Commissioner**

**15 September 2016**

## Appendix 1: Relevant statutory provisions

---

### Freedom of Information (Scotland) Act 2002

#### 1 General entitlement

(1) A person who requests information from a Scottish public authority which holds it is entitled to be given it by the authority.

...

(4) The information to be given by the authority is that held by it at the time the request is received, except that, subject to subsection (5), any amendment or deletion which would have been made, regardless of the receipt of the request, between that time and the time it gives the information may be made before the information is given.

...

(6) This section is subject to sections 2, 9, 12 and 14.

#### 2 Effect of exemptions

(1) To information which is exempt information by virtue of any provision of Part 2, section 1 applies only to the extent that –

...

(b) in all the circumstances of the case, the public interest in disclosing the information is not outweighed by that in maintaining the exemption.

...

#### 17 Notice that information is not held

(1) Where-

(a) a Scottish public authority receives a request which would require it either-

(i) to comply with section 1(1); or

(ii) to determine any question arising by virtue of paragraph (a) or (b) of section 2(1),

if it held the information to which the request relates; but

(b) the authority does not hold that information,

it must, within the time allowed by or by virtue of section 10 for complying with the request, give the applicant notice in writing that it does not hold it.

...

**30 Prejudice to effective conduct of public affairs**

Information is exempt information if its disclosure under this Act-

...

- (c) would otherwise prejudice substantially, or be likely to prejudice substantially, the effective conduct of public affairs.

**35 Law enforcement**

- (1) Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice substantially-

- (a) the prevention or detection of crime;
- (b) the apprehension or prosecution of offenders;

...

## Appendix 2: Mr Tibbitt's request of 9 June 2015

---

### Freedom of Information Request: Compliance with CCTV regulations

Please could you provide me with the following information:

1. A copy of the current Community Safety Glasgow CCTV Local Code of Practice in electronic format.
2. A copy of the current Community Safety Glasgow CCTV Local Operations Manual in electronic format.
3. A copy of the local Intrusive Surveillance procedures in electronic format.
4. Copies of any current written agreements that permit secondary monitoring of Community Safety Glasgow CCTV cameras.
5. A copy of the Deployment Criteria which Community Safety Glasgow uses to govern the use of re-deployable CCTV cameras.
6. Copies of the last three annual reports produced by Community Safety Glasgow on its CCTV system.
7. Copies of the last two System Evaluations that Community Safety Glasgow has carried out on its CCTV system.
8. Confirmation of the number of times the Community Safety Glasgow CCTV system has been operated partially, or fully, by a third party organisation in the last three years. For each occurrence, if any, please confirm which third party agency took over control (or partial control) of the system, when control was given, and for how long.
9. A copy of the most recent report made by Community Safety Glasgow to the Surveillance Camera Commissioner.

If possible, I would prefer to receive this information in an electronic, machine readable format, such as Microsoft Word or Excel. I would prefer not to receive these documents in pdf format if possible.

**Scottish Information Commissioner**

Kinburn Castle  
Doubledykes Road  
St Andrews, Fife  
KY16 9DS

t 01334 464610

f 01334 464611

[enquiries@itspublicknowledge.info](mailto:enquiries@itspublicknowledge.info)

**[www.itspublicknowledge.info](http://www.itspublicknowledge.info)**