The Information Commissioner's view on the provisions of the Protection of Freedoms Bill
As at Committee Stage (House of Lords)

Introduction

1. The Information Commissioner has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA). The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

2. The Information Commissioner welcomes many of the provisions contained in the Protection of Freedoms Bill. His office has been consulted early and regularly on several of the proposals. The clarity that these proposals will bring is to be welcomed and in some respects provide greater transparency and protection for privacy. The Bill also makes welcome provision for increasing the independence of the Information Commissioner.

3. This evidence will be limited to those areas that fall within the Information Commissioner's regulatory remit. These areas include:
   - Part one, chapter one, destruction, retention and use of fingerprints etc. (paragraphs four to 18);
   - Part one, chapter two, protection of biometric information of children in schools (paragraphs 19 to 22);
   - Part two, chapter one, regulation of CCTV and other surveillance camera technology (paragraphs 23 to 32);
   - Part three, chapter two (including Schedule 4), vehicles left on land (paragraphs 33 to 36);
   - Part five, general comments (paragraphs 37 to 42);
   - chapter one, safeguarding vulnerable groups (paragraphs 43 to 47);
   - Part five, chapter two, criminal records (paragraphs 48 to 55);
   - Part five, chapter three, disregarding certain convictions for buggery etc. (paragraphs 56 to 58); and
   - Part six, Freedom of Information and Data Protection (paragraphs 59 to 74).

Part one, Chapter one – destruction, retention and use of fingerprints etc.

4. The Commissioner welcomes specific provisions limiting how long biometric information can be retained by the police on those individuals who are of no ongoing concern. The Commissioner's view is that an evidence based approach should be adopted taking into account the decreasing value of older records over time. However, these provisions are a significant improvement erring on the side of greater privacy protection.

5. The Commissioner is concerned that although there is provision to delete fingerprints and DNA profiles there does not appear to be a provision to delete the allied biographical information, as in the arrest record, contained on either Police National Computer (PNC) or Police National Database (PND). It is clear that when a DNA profile is created and loaded onto the national DNA database an identity record relating to the arrest from which the DNA sample was obtained is automatically created on the PNC. What is not clear is whether this PNC record is also deleted when the DNA profile is removed from the national DNA database.

6. At present all records held on the PNC are readily accessible to serving police officers and other police staff acting in their official capacity and this access is frequently used to run a "name check" on individuals who come into contact with the police. Given this level of access, the very existence of a PNC identity record created as a result of a biometric sample being taken on arrest could prejudice the interests of the individual to whom it relates by creating inaccurate assumptions about his or her criminal past when that record is accessed.

7. The Information Commissioner believes that there is no justification for the police to continue to retain a PNC identity record which is linked to other biometric records that the police are required to delete having served their purpose. This engages concerns about compliance with the fifth principle of the DPA in that personal data should not be kept for longer than necessary. In the Commissioner's view the Bill should include clear provisions requiring the deletion of all such associated records when fingerprints and DNA are deleted.

8. A number of clauses, such as clauses 3 (2), 4 (2), 5 (2), 6(3), 7(3) and (5), and 10(3) permit, continued retention of material in specified circumstances. The clauses as drafted then permit indefinite retention. This appears to be irrespective of any ongoing necessity for crime prevention and detection purposes. It would be consistent with the requirements of the fifth principle of the DPA to amend this to permit retention for as long as is necessary for the prevention and detection of crime, the investigation of an offence or the conduct of a prosecution. This construction has

been used in clause 15(3) when dealing with footwear impressions and more closely accords with the requirements of the DPA.

9. The Commissioner is concerned that there is no facility available for individuals to request deletion of their DNA and fingerprints. Also, there is no independent appeal process for those individuals whose DNA and fingerprints the Chief Officer may have refused to destroy in connection with this section and consideration should be given to this.

10. Clause one also provides that a speculative search can be undertaken 'within such time as may reasonably be required for the search if the responsible chief officer of police considers the search to be desirable'. It appears that this power as drafted would permit a search to be undertaken after Section 63D material has been determined to be unlawful or after consent has been withdrawn. The explanatory notes to the Bill explain that this clause 'enables a person's Section 63D material, which would otherwise fall to be destroyed, to be retained for a short period until a speculative search of the relevant databases has been carried out'. The notes say that where such a match occurs it might serve to confirm the person's identity, indicate that he or she had previously been arrested under a different name or indicate that the person might be linked to a crime scene from which fingerprints or a DNA sample had been taken. The provision in this clause is wide and would mean that a speculative search could be done in every case. In principle, a speculative search should only be undertaken on material deemed to be unlawful or where consent has been withdrawn when there is a pressing need to do so. It is not clear that the case has been made for this and nor is it clear what a short period for retaining the material would be. Undertaking speculative searches without justification after material is deemed to be unlawful or after consent has been withdrawn could engage concerns about compliance with the fair and lawful processing requirements of the DPA.

11. Clause two provides for the retention of fingerprints and DNA "until the conclusion of the investigation of the offence or, where the investigation gives rise to proceedings against the person for the offence, until the conclusion of those proceedings". The Commissioner would welcome more clarity in the wording of paragraph (2) of Section 63E and in particular in the phrase "until the conclusion of the investigation" to ensure there are no circumstances where categorisation as an un-concluded investigation justifies retention even though the police have no ongoing concerns about criminal activity.

12. Clause 10 deals with material given voluntarily. This provides for material being retained until it has fulfilled the purpose for which it was taken although it may be retained indefinitely if the individual is or has been convicted of a recordable offence. It should be a requirement that individuals are told of the potential

consequences of giving material voluntarily and that the material may be retained indefinitely in some circumstances.

13. Clause 13 refers to the destruction of DNA profiles and that no copy must be retained by the police except in a form which does not include information which identifies the person to whom the DNA profile relates. It is assumed that this is aimed at addressing issues relating to the raw data, the electro-phoretogram, from which the DNA profile is created. Historically, difficulties have arisen with the destruction of individual electro-phoretograms as these are, in some cases, processed in batches. This provision should be expressed in a way so it cannot be used to perpetuate such batch processing practices in any new systems used to generate DNA profiles and to require deletion of all the DNA profile information as the norm and retention in an anonymised form only as an exceptional circumstance.

14. Clause 14 refers to samples being destroyed immediately if it appears to the responsible chief officer of police that 'the taking of the samples was unlawful, or the samples were taken from a person in connection with that person's arrest and the arrest was unlawful or based on mistaken identity'. Again there is reference here (at (6)) that a speculative search can be carried out 'within such time as may reasonably be required for the search if the responsible chief officer of police considers the search to be desirable'.

15. Clause 15 relates to impressions of footwear. Although footwear impressions may not engage the same level of privacy concerns as biometric material, safeguards need to be in place such as ensuring other information is not retained longer than the impressions when a person is of no ongoing interest including the nominal information on the PNC.

16. Clause 20(6) specifies the functions of the Commissioner for the Retention and Use of Biometric Material. There may be some overlap between the respective functions of the Commissioner for the Retention and Use of Biometric Material and the Information Commissioner in relation to the processing of biometric material and it is important that the Commissioners work closely together in any such circumstances.

17. The explanatory notes in relation to Clause 23 refer to the National DNA Database (NDNAD) being maintained and operated by the National Policing Improvement Agency (NPIA). Consideration will need to be given to management of this database with the phasing out of the NPIA to ensure that the database is effectively managed in the future.

18. Clause 24 details the formation and responsibilities of the National DNA Database Strategy Board. The creation of a Board is welcome but the composition of the Board is not specified on the face of

the legislation. It is important that this is clarified to ensure that the membership is appropriate for the functions it is meant to perform and that there are other interests reflected in the composition of the Board rather than just comprising of representatives of the law enforcement community.

Part one, chapter two – protection of biometric information of children in schools

19. Processing biometric information about a child is an intrusive activity that can be a source of concern to children and parents. The Commissioner considers parental consent provides the best legal basis for doing this, although the DPA can provide alternatives in some circumstances. The adoption of this measure would also clear up the considerable legal uncertainty faced by schools in determining whether or not they need parental consent to produce a biometric, from a child's finger-print or other biological measurement.

20. It is clear that a child can overrule a parent by refusing to participate in anything that involves the processing of his or her biometric information. However, it is not clear whether this means that a child should also be able to overrule a parental decision *not* to allow participation. In other words, if a parent refuses to allow their child's biometrics to be processed, can the child overrule this decision? The Bill as it stands is not clear on this point.

21. Clause 27 provides exceptions to the requirement to obtain parental consent. Clause 27(d) provides that parental consent is not required where "it is otherwise not reasonably practicable to obtain the consent of the parent". Such a broad exception to the requirement to obtain consent may bring further confusion and less certainty for parents and children. For example, will a school that already processes biometric information of children that was collected without parental consent now have to obtain consent and provide alternative means of participation for children? Or will having to do this retrospectively, with all the potential expense or administrative burden this may entail, mean that it is "not reasonably practicable to obtain the consent of the parent"?

22. Clause 28 provides a definition of 'biometric information'. The definition as it stands is considerably broader than that in general use, where a biometric is generally defined as a metric produced from a biological measurement. The definition 'biometric information', as it currently stands in the Bill, could apply to various sorts of information – for example a photograph on a bus-pass - that are not generally considered to be biometrical. While clause 28(1)(3) clarifies the type of information that clause 26 is meant to apply to, there is still potential for confusion with the more general definition of 'biometric information'.

Part two, chapter one - regulation of CCTV and other surveillance camera technology

23. The Information Commissioner is keen to see effective regulation of CCTV and automatic number plate recognition (ANPR) systems and other emerging camera technologies. Ensuring camera surveillance is subject to effective control is essential and the Commissioner supports government efforts to drive up standards and to regulate further in this important area. The DPA will still apply where images and ANPR data are related to individuals and across all sectors throughout the UK. It is important that the proposed regulatory approach is consistent with these requirements, enhances safeguards and does not lead to confusion. It is very welcome that the government has made it clear that nothing in the Protection of Freedoms Bill in relation to the regulation of surveillance camera systems will interfere with the current role and responsibilities of the Information Commissioner and the DPA will continue to have primacy as it applies to the processing of personal data by surveillance camera systems. This is a welcome clarification and it would be helpful to have this reflected in the proposed code.

24. The Bill requires the Secretary of State to prepare a code of practice containing guidance about surveillance camera systems. According to Clause 29 the code must contain guidance about the use or processing of images or other information obtained by such systems and "processing" has the meaning given by section (1) of the DPA. The Information Commissioner welcomes the provision that he must be consulted by the Secretary of State in the course of preparing the code. As the UK's independent authority upholding information rights, the Information Commissioner is keen to ensure the provisions of the code are consistent with and complement existing data protection safeguards and do not lead to any confusion over what regulatory requirements apply in practice in all sectors across the UK. This is particularly true in relation to the Information Commissioner's own existing published CCTV code of practice which helps organisations comply with the legal requirements of the DPA and adopt good practice standards.

25. It is important that any new regulations follow the better regulation principles and are transparent, accountable, proportionate, consistent and targeted at cases where action is needed. It is essential that surveillance camera operators understand that they must comply with the legally enforceable provisions of the DPA even though they may not be obliged to follow the Secretary of State's code. Individuals must also be clear about how to exercise their rights in relation to the DPA, for example, their right to ask to view and have copies of images of themselves.

26. The Information Commissioner welcomes the requirement to be consulted by the Secretary of State on the provisions of the proposed code and he will use this opportunity to try to ensure

they reflect the requirements of existing data protection law. But it will be a significant challenge to try to reconcile different legislative approaches within one document, especially where there are differences in territorial scope, sectors covered, compliance obligations and enforcement mechanisms. In addition the Information Commissioner is able to deal with matters that relate to data generated or used, particularly in connection with ANPR, where existing databases are consulted and where vehicle movement details are recorded in databases for future use. The development of automatic facial recognition will also engage similar issues of ensuring appropriate supervision of all personal data in closely related contexts. The Information Commissioner would not want to see any weakening of data protection safeguards but wants to help ensure that any new arrangements enhance the work the ICO has done already in setting good practice data handling standards for CCTV system operators.

27. The Information Commissioner welcomes the Bill's wide focus on "surveillance camera systems" and its specific references to closed circuit television and automatic number plate recognition systems. The Commissioner is pleased that the government has taken up his suggestion that the definition of these systems in Clause 29 (6)(b) is simplified and it now refers to "any other systems for recording or viewing visual images for surveillance purposes".

28. The Information Commissioner is concerned that only the police and local government will be obliged to follow the proposed code, at least initially. This could cause problems in practice given the many partnership arrangements between the public and private sectors for town centre monitoring. There is also widespread use of CCTV and ANPR systems across all sectors including government agencies and increasing deployment of ANPR in the private sector such as with car park operation, where sometimes details of people's vehicle movements are stored indefinitely and insufficient safeguards are in place regarding security, access and further use. The Information Commissioner considers further thought should be given to the implications of limiting the obligation to give "due regard" to the code to just the police and local government. At the very least it should consider extending the scope of the code to include central government departments and their agencies, especially those with significant usage or involvement with camera systems such as the Department for Transport and the Home Office.

29. There is no mechanism in the Bill for direct enforcement of the code or for dealing with individual complaints about non compliance with the code. It is not clear whether the Information Commissioner's existing powers to handle complaints and take enforcement action concerning breaches of the DPA have any role to play. How these issues are to be handled in practice needs clarifying.

30. The government has indicated that the role and responsibilities of the new Surveillance Camera Commissioner will complement but be distinct from those of the Information Commissioner and there will be a strong degree of mutual interest. The Information Commissioner is fully committed to working with the Surveillance Camera Commissioner and is keen to help ensure there is effective regulatory oversight of surveillance camera systems across the UK, following better regulation principles. It is essential that all the commissioners who have a role in overseeing camera surveillance have clear and complementary roles as part of a transparent and consistent regulatory framework.

31. The Surveillance Camera Commissioner's functions include encouraging compliance with and reviewing the operation of the surveillance camera code. In addition, Clause 34 (2) states that the Surveillance Camera Commissioner will provide advice about the code (including changes to it or breaches of it). As the Bill stands this presumably includes providing advice about the processing of personal information if it is covered by the provisions in the code. It will be important to clarify the roles of the respective commissioners because, as the Bill stands, there will be overlaps in their responsibilities running the risk that commissioners may adopt differing interpretive approaches and guidance on each others' statutory provisions with the risk of regulatory confusion.

32. Further details of the Information Commissioner's views on the regulation of CCTV and ANPR can be found in his detailed response to the Home Office's consultation on the Surveillance Camera Code which closed on 25 May 2011. The response is available on our website (http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx)

Part three, chapter two – vehicles left on land

33. At the Commons Report Stage, government amendments were approved which extend the application of the keeper liability regime to circumstances where an obligation to pay a parking charge arises as a result of parking on private land. The amendments also allow the use of CCTV or automatic number plate recognition (ANPR), as well as the physical ticketing of vehicles, in order to manage parking on relevant land. The ICO does receive complaints from vehicle owners who have received retrospective parking charge notices from car park operators who have often used CCTV and ANPR technology to identify vehicles which have contravened their parking rules. Complaints centre on lack of signage and inaccuracy of the ANPR reads.

34. The Information Commissioner has concerns that the Bill will encourage increasing use of a powerful surveillance technology by unregulated car park operators. It is clear from complaints to his

office that ANPR data is not always subject to proper information governance and insufficient safeguards are in place to ensure the information is kept securely and vehicle keeper records are checked properly to ensure they are accurate and up to date. The Information Commissioner would not want to see rogue wheel clampers becoming rogue ANPR operators. Nor does he want increased use of ANPR to lead to greater access to DVLA vehicle keeper data without robust safeguards to ensure that there is no risk of abuse by those who seek to find out details of vehicle keepers for other reasons. The Information Commissioner also has concerns about the potential for misreads if car park cameras are positioned incorrectly or used in adverse conditions and the impact this will have on vehicle keepers. No ANPR system is 100% accurate and care must be taken to check the ANPR reads against the visual image of the number plate.

35. The Information Commissioner is also aware that private car parking organisations are building up large collections of ANPR "read" data and sometimes are retaining this data indefinitely. Lengthy or indefinite retention of all ANPR data reads is inappropriate for managing a car park.

36. Clearly some information on these databases can be a valuable resource for police forces investigating crimes but use of this information must comply with the requirements of the Data Protection Act. The Information Commissioner has concerns about car park operators and police sharing information about "vehicles of interest" without sufficient security and contractual arrangements in place. In the absence of a statutory basis for unlimited police use and mass sharing of private sector ANPR data, the Information Commissioner will be reminding the parties involved that they must be able to justify collection and sharing of ANPR data in each particular case. He will also continue to advise the police that any proposals to share third parties' ANPR data should be based on a pressing need and must be subject to adequate safeguards. It will be important to ensure that the Home Secretary's code and the approach of the Surveillance Camera Commissioner are aligned with this work.

Part five - safeguarding vulnerable groups, criminal records etc

37. The Commissioner recognises the importance of a Vetting and Barring Scheme and criminal record disclosure service that strikes the right balance between protecting vulnerable members of society and the rights of ex-offenders to rehabilitation. It is important that there are adequate safeguards in place to prevent inappropriate individuals working with or having unsupervised access to children or vulnerable adults however those safeguards should be proportionate and fair. The Commissioner considers that overall the provisions in the Protection of Freedoms Bill take a positive step towards achieving that balance.

38. The Commissioner shares some concerns which have also been identified in the Independent Advisor for Criminality Information Management's report 'A Common Sense Approach' and which have not been included in the legislation. There does not appear to be any specific provisions to:

- filter to remove old and minor conviction information from criminal records checks;
- ensure penalties and sanctions for employers knowingly making unlawful criminal records checks are rigorously enforced; or
- to introduce basic level criminal record checks in England and Wales.

39. The Commissioner believes that criminal records certificates should only include relevant conviction information and supports the recommendation in the Independent Advisor for Criminality Information Management's review to introduce a filter to remove old and minor conviction information. The onus should not be on the individual to disclose old or minor conviction or caution information to a potential employer where it is irrelevant and excessive in relation to the job role. This could lead to a disproportionate effect on the applicant if taken into account in the employment decision. Both the legislation and any guidance on this matter should, if possible, put this issue beyond doubt.

40. Criminal records disclosure bodies should have processes in place to ensure that standard and enhanced certificates are only issued where a position is covered by the Rehabilitation of Offenders Act 1974 (Exceptions Order) 1975. The Commissioner is unclear whether such procedures will be implemented and, if an employer is found to be knowingly making unlawful criminal records checks, how penalties and sanctions will be rigorously enforced.

41. The introduction of basic disclosures would provide a more privacy friendly and proportionate way of providing prospective employers with unspent conviction information, or confirmation that there is no such information, with important safeguards in place. This will require section 112 of the Police Act 1997 to be commenced.

42. The Commissioner is also concerned that the scaling back of the Vetting and Barring Scheme could lead to an increase in 'enforced subject access'. Bodies who will have been able to undertake criminal records checks may not be able to now and these bodies could potentially require the individual to make a subject access request to obtain that conviction information. This makes it even more important that the existing but as yet unimplemented offence provisions aimed at dealing with Enforced Subject Access are implemented as a vital safeguard to prevent employers circumventing the Rehabilitation of Offenders Act 1974 and the criminal records disclosure regime. This measure to prevent individuals' rights being misused has been lacking for a number of years. Without the introduction of sanctions to deal with Enforced

Subject Access the criminal record disclosure regime will continue to be undermined. To ensure that this is not the case this will require commencement of section 56 of the Data Protection Act 1998 and the relevant provisions in Part V of the Police Act 1997.

Part five, chapter one - safeguarding of vulnerable Groups

43. The Commissioner welcomes the scaling back of the Vetting and Barring Scheme. Whilst it is recognised that there needs to be safeguards in place to protect the most vulnerable members of our society, this needs to be proportionate. The Commissioner therefore welcomes many of the amendments to the scheme which he considers will, in effect, lead to a more proportionate mechanism for protecting society's most vulnerable.

44. The Commissioner welcomes Clause 72 which repeals the facility for employers and others to register a legitimate interest in an individual without their knowledge. This meant that those interested parties would be informed if someone was barred and this was specifically in relation to individuals who were subject to monitoring. This provision had meant that employers or other interested parties who may no longer have been relevant would have been updated on an individual's circumstances.

45. The new provision means that it is only an interested party who, on application, could obtain that information and it would be with the individual's consent or authorisation to do so. While the Commissioner welcomes the limitation on who can obtain information, introducing a consent model for the disclosure of this information could be problematic. Consent in a data protection framework needs to be specific, informed and freely given. Not giving consent in this situation could have a detrimental impact on the individual and therefore could call into question whether the consent has not been freely given. Further, if an individual has consented to the disclosure of this information then they will be within their rights to withdraw that consent at any time. To refuse consent in this situation will or could be detrimental to the individual and engages concerns whether there is potential to place an individual under undue duress to provide consent in this situation. The Commissioner understands why the consent model has been introduced but consideration will need to be given as to whether this is an appropriate model to rely on in practice.

46. There is still a facility to register an interest in an individual to be advised if that individual becomes barred from regulated activity but that would be with the individual's consent/knowledge.

47. Clause 73 ensures there will now be a requirement on employers or agencies to check whether an individual applying to engage in a regulated activity is on a barred list. One of three steps can be taken to ensure that the employer/agency's obligations have been met which include updates being provided which indicate that the

individual is not barred (with the individual's consent), the employer has obtained an enhanced CRB check or the employer has received up to date information in relation to that certificate. This is welcome as it essentially means that if an individual does not consent then the employer/agency can still undertake a check to meet their obligation without placing an individual under duress to provide consent.

Part five, chapter two - criminal records

48. The Commissioner welcomes provisions in Clause 79 to make individuals responsible for providing the registered person with their criminal record disclosure certificate rather than it being sent directly to the registered person (the employer or its representative). This will ensure that individuals can review and challenge any inaccurate information included on the certificate before it is disclosed to the registered person. This should avoid any detriment caused to an individual by inaccurate information included on a certificate. However, a robust and timely dispute process is essential to this provision having the required practical effect. Any delay in an individual providing a certificate to the registered person could lead to unfair inferences. The Commissioner is concerned that there are no timescales for the dispute process specified in the Bill. This would reduce the likelihood of an individual losing an employment opportunity due to a delay caused by inaccurate information.

49. The Commissioner welcomes the introduction of a higher test to be applied by a chief police officer when deciding whether 'other relevant information' should be included on an enhanced certificate in Clause 81. The Commissioner considers that when making a decision as to whether information 'ought' to be included on the certificate the chief police officer must give equal weight to the social need to protect vulnerable members of society and the applicant's right to respect for private life. This is supported by Lord Hope, who stated in R (on the application of L) (FC) (Appellant) v Commissioner of Police of the Metropolis (Respondent), [2009] UKSC 3 "The correct approach, as in other cases where competing Convention rights are in issue, is that neither consideration has precedence over the other." The Secretary of State's guidance, which the chief police officer must have regard to, should put this issue beyond doubt.

50. The Commissioner supports the introduction of provisions to update certificates in Clause 82. This will ensure the "relevant person" does not receive the new information before the individual and the individual has an opportunity to challenge the accuracy of the information. There is a concern about the update process and some important safeguards may be lacking.

51. The inclusion of "any person authorised by the individual" in the definition of "relevant person" for criminal conviction certificates,

criminal record certificates and enhanced criminal record certificates needs careful consideration. There is potential for an individual to be put under undue duress to be subject to up-date arrangements. There should be a robust procedure in place to ensure that for criminal record certificates and enhanced criminal record certificates, the "relevant person" is only asking for the update arrangements to be in place for the purposes of an exempted question.

52. If an individual moves from a position that requires an enhanced criminal record certificate to a position that requires only a criminal record certificate there is a potential for the individual to be providing a higher level of disclosure than the job role requires. This is especially the case if moving between the two levels of disclosure subject to the up-date provisions has a financial implication for the individual. The regulations prescribing fees should allow an individual to move to a lower level of disclosure without a financial cost to ensure they do not disclose more information than is necessary for the job role.

Clause 84

53. The commencement of section 112 of the Police Act 1997 would be welcome. The Commissioner would also continue to stress the importance of introducing an offence of Enforced Subject Access under section 56 of the Data Protection Act as a matter of urgency. The opportunity to introduce these important and long over due measures should not be missed.

54. If section 112 Police Act 1997 is to be commenced the effect of the proposed amendment to include conditional cautions on basic criminal conviction certificates should be considered. Given the short three month rehabilitation period for conditional cautions under the Rehabilitation of Offenders Act 1974 (as amended by the Criminal Justice and Immigration Act 2008), after which time they become spent, the Commissioner would question whether it is proportionate for conditional cautions to be included on a basic criminal conviction certificate.

55. The disclosure of this information could lead to the individual being denied an employment opportunity. Had the individual applied for the same position once the conditional caution became spent, which could be between one day and three months later depending on the time of the job application, the conditional caution would not be disclosed to the prospective employer. Given that the condition caution is designed to rehabilitate the offender, or provide reparation to the victim, careful consideration should be given as to whether the disclosure of this information, and the potential loss of an employment opportunity, is appropriate.

Part five, chapter four - disregarding certain convictions for buggery etc.

56. The Commissioner supports provisions to allow convictions or cautions for homosexual acts, where those acts would no longer be an offence, to be disregarded by the Secretary of State. However, these provisions could be substantially improved in two important respects.

57. Firstly, all of these convictions or cautions should be disregarded automatically rather than relying on the person who was convicted, or cautioned, to make an application to the Secretary of State. Police Forces should not be holding irrelevant or excessive personal data about individuals. If information relating to these offences is no longer relevant it should not be retained.

58. The definition of 'delete' does not follow its natural meaning. Many would assume that this is equivalent to 'erasure' of a record. Records are not in fact 'deleted' but a retained record is annotated with the fact that it is to be disregarded. This is unnecessarily confusing and the term 'delete' should not be used to describe what happens to the record. It is not clear why such an approach has been adopted and if a record relates to a person and conviction where there is no ongoing police interest over time the conviction should be erased. This approach would accord with the requirements of the fifth data protection principle which requires that personal data are held for no longer than necessary for their purpose. Further, this links in to our concerns outlined in paragraph six above and the resulting risk of prejudice to individuals given that the information is not in fact deleted.

Part six - Freedom of Information and Data Protection

59. The Commissioner welcomes the changes proposed to the Freedom Of Information Act (FOIA), which offer new rights to request datasets in open formats which will also be available for re-use under a specified licence. The changes to the FOIA publication scheme provisions, adding a requirement to publish requested datasets, when appropriate, are also welcome amendments. The Commissioner believes that is important that these changes are implemented via the statutory scheme of the FOIA and will therefore be enforced by the Commissioner with his other FOI functions. The time is also right to consider greater convergence between legal provisions on access and re-use.

60. It is important that the FOIA is updated to take account of new possibilities to promote openness using internet technologies. This has been described as FOI 2.0. It is clear that the possibilities of requesting and re-using datasets were not envisaged when the Act was drafted. The Commissioner has been impressed by recent initiatives by the public sector to open up public sector datasets on topics such as public spending and crime data. He has also been impressed by the innovative uses of datasets made by a range of public data projects, some by NGOs and charities, and

other uses by commercial organisations and newspapers. Many of the new websites and services that use the data are very user friendly and generally accessible to the public.

61. The proposed changes are welcome because they should lead to greater openness and transparency, enabling citizens to understand more about the work of public authorities and hold them to account. The Commissioner has long held the view that proactive disclosure is a key component in delivering transparent and open government. Levels of trust will build incrementally from a sustained programme of proactive disclosure. Trust will also build from an open approach to disclosing information in response to Freedom of Information requests, taking an approach that builds on the assumption in the favour of disclosure that is build into the Act.

62. The changes to sections 11, 19 and 45 of FOIA proposed in clause 100 are positive but the Commissioner offers the following observations.

63. The definition of dataset proposed should be workable but it should be monitored closely during early periods of operation, to ensure that public bodies do not use the proposed definition in section 11(1A) too narrowly, in particular how they apply the provision that excludes factual information "which is not the product of analysis or interpretation, other than calculation".

64. It is also important that further clarification is provided around the meaning of section 19(2A): "unless the authority is satisfied that it is not appropriate for the dataset to be published." The Commissioner presumes this to mean that "not appropriate" may include the circumstances where the requested dataset is withheld under an exemption. However, this may not be the case if the passage of time or other circumstances change between the request being made and publication is considered. The Commissioner also suggests that the changes to section 19 could go further to ensure that there is general obligation on public authorities to include datasets in their publication schemes, regardless of whether a request has been made. This would give the Commissioner greater authority to include classes related to datasets in any model schemes and guidance prepared by him under section 20 of FOIA. Changes to section 20 of FOIA may also be required to enable a proactive approach to disclosure of datasets.

65. The Commissioner will consult about how publication schemes can be implemented in light of any dataset related amendments to FOIA and how any wider demands for information from publication schemes can be met. The Commissioner is also mindful that any implementation needs to be sustainable and take account of resources available in public authorities.

66. This clause introduces the provision for a public authority to charge a fee. The Commissioner understands the need for charging for re-use for certain datasets but guidance should make clear that charging should not be the default.

67. The Commissioner acknowledges that certain aspects of the changes proposed in clause 100 will become clearer when the proposed changes to the section 45 Code of Practice are published.

68. Provisions related to copyright in the proposed section 11A of FOIA could be extended further, beyond datasets. However, the Commissioner acknowledges that an opportunity may also be available to consider this issue during the post legislative scrutiny recently announced by the Ministry of Justice[1].

69. It is also important the regime for accessing Environmental Information - the Environmental Information Regulations 2004[2], also benefits from the changes proposed in clause 92. The Commissioner considers that this is important as access to environmental information is a matter of significant public interest and these rights should not fall behind other rights. The INPSIRE Regulations[3], passed in 2009 do implement some obligations for public authorities to publish environmental information but not comprehensively. The Commissioner acknowledges there could be some difficulty in aligning these two environmental regimes with the changes proposed in the Bill, as the two regimes are derived from European Directives[4]. However, given the progressive nature of the amendments in this Bill it does not appear that any alignment could be seen as posing a risk of weakening the implementation of the transposition. The INPSIRE Directive clearly points to the European intention in area, to open up public data on open formats.

70. In clause 101, the changes proposed to section 6 of FOIA are welcomed by the Commissioner and will bring wider accountability and transparency to bodies that are receiving significant public funds, are subject to public sector control and/or are delivering important services to members of the public.

71. The Commissioner suggests that the term "wider public sector" is unclear and there is a strong need to give legal clarity to the term. The Commissioner does not believe it would be in the

---

[1] http://www.justice.gov.uk/news/newsrelease070111a.htm
[2] The Environmental Information Regulations 2004 3391
[3] The INSPIRE Regulations 2009 SI 3157
[4] Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE).

public interest for this clarity on interpretation to emerge via section 50 complaints to his office, appeals to the First-tier and Upper Tribunal, and the Higher Courts, which could prove to be very costly. The Commissioner is not aware of this term being used in other relevant legislation that may offer guidance. To ensure that these changes have real effect the term should be defined in the legislation.

72. Clauses 103 to 106 of the Protection of Freedoms Bill seek to further enhance the Commissioner's day-to-day corporate and administrative independence. They will mean that the Commissioner will no longer need to seek the consent of the Justice Secretary on issues relating to staff appointments, charging for certain services, or before issuing certain statutory codes of practice under the DPA.

73. In addition, changes are also being made to the terms of the Commissioner's appointment and tenure to increase transparency and protect against any potential undue influence. The Commissioner fully supports the intention behind this proposal and in particular the idea that future commissioners are appointed for a fixed term of office of seven years that is not renewable. All the previous post-holders have had their initial five year terms extended to varying degrees and this has helped ensure continuity in the work of the Information Commissioner's Office and enabled each Commissioner to develop and implement a long term approach to information rights regulation.

74. The measures are underpinned by a revised Framework Document which outlines the day-to-day relationship between Government and the Information Commissioner. The Ministry of Justice consulted with the ICO over the nature of the proposed changes and the specific clauses and the ICO fully supports the changes as a helpful move to reinforce the Commissioner's independence from government. This independence is necessary if the Commissioner is to fulfil his roles defined in FOIA and DPA. http://www.ico.gov.uk/about_us/how_we_work/relationship_with_moj.aspx

23 November 2011