The Information Commissioner's evidence to

The Public Bill Committee

On the Protection of Freedoms Bill

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. There is potential for confusion between some the provisions of this Bill and legislation within the Information Commissioner's regulatory competence. There are also areas where there is potential for overlap between the roles and functions of the Information Commissioner and others set out in the in the Bill. On other points, there is a lack of detail and potential for confusion over the substance of the Bill itself. Some of these provisions may have benefited from more detailed consultation with the Information Commissioner during their development to ensure greater clarity from the outset.

4. 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 five to 19);
    - Part one, chapter two, protection of biometric information of children in schools (paragraphs 20 to 24);
    - Part two, chapter one, regulation of CCTV and other surveillance camera technology (paragraphs 25 to 34);
    - Part three, chapter two (including Schedule 4), vehicles left on land (paragraphs 35 to 40);
    - Part five, general comments (paragraphs 41 to 46);
    - chapter one, safeguarding vulnerable groups (paragraphs 47 to 51);
    - Part five, chapter two, criminal records (paragraphs 52 to 61);
    - Part five, chapter three, disregarding certain convictions for buggery etc. (paragraphs 62 to 65); and
    - Part six, Freedom of Information and Data Protection (paragraphs 66 to 80).

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

5. 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 whereby necessity is considered taking into account the value of these records over time. However, these provisions are a significant improvement erring on the side of greater privacy protection.

6. 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.

7. At present all records held on the PNC are readily accessible to any serving police officer acting in his or her 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.

8. 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 Data Protection Act 1998. 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.

9. Clause one outlines the circumstances in which a chief officer must order the destruction of the fingerprints or DNA profiles. Broadly these are when the taking of fingerprints or DNA was unlawful or the related arrest was unlawful or based on mistaken identity. There are other circumstances in which the Chief Officer could order destruction of the fingerprints or DNA which do not appear in the Bill, such as where there is a legal duty to comply with other relevant pieces of legislation such as the DPA or the Human Rights Act in relation to the circumstances relating to the arrest, the nature of the alleged offence

or the retention of the fingerprints or DNA. Parliament could give consideration to including an additional circumstance in the criteria for destruction where this is to discharge such a legal obligation.

10. Including such an additional ground for deletion in this Section would also help ensure that there is no ambiguity in the interpretation of other aspects of these provisions. In the past during discussions with the police on the exiting provisions regarding the retention of DNA profiles the word "may" in relation to retention has been taken to be a strict requirement to retain for an indefinite period.

11. 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.

12. 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.

13. In Clause three, amendment Section 63F (5) refers to fingerprints and DNA taken from a person who is charged with but not convicted of a qualifying offence which can be retained for three years (with a possible extension by a further two years) if, amongst other things, "any prescribed circumstances apply" (63F (5c)). Paragraph 11 of Section 63F makes it clear that the prescribed circumstances must include the fact that the Commissioner (for the Retention and Use of Biometric Material) ('the Biometric Commissioner') has consented to the retention of the material (fingerprints and DNA). In addition, Paragraph 12 provides an order making power for the Secretary of State to prescribe the circumstances which "may make provision about the procedure to be followed in relation to any decision of the Commissioner and an appeal against such a decision". Clearly until an order is made under 63F (12) the exact details of all the prescribed circumstances will not be clear.

14. However, Clause 20 of the Bill makes it clear that the functions of the Biometric Commissioner are all to do with matters of national security. In view of this it is not clear why, according to 63F (11), the Biometric Commissioner must consent to the retention of material relating to any qualifying offence not just material that relates to qualifying offences to do with matters of national security. This seems to extend the functions of the Biometric Commissioner beyond matters of national security.

15. It is also not clear who the right of appeal in 63f (12) relates to. This appears to be a right of appeal against the Biometric Commissioner's decision to retain material so presumably the appeal relates to the person from whom the material is taken. This requires clarification as does the role and function of the Commissioner in relation to this part of the Bill.

16. Clauses 10 and 11 deal with material given voluntarily and material retained with consent. The explanatory notes say that the provision in Clause 11 that allows for the retention of such material as long as the person consents also applies to Clause 10 and that this consent "must be in writing and can be withdrawn at any time". Where the confusion arises is that Clause 10 refers to "material given voluntarily" (which is mainly about material used for elimination purposes) makes it clear that such material "may be retained until it has fulfilled the purpose for which it was taken or derived". This is confusing and requires clarification as if the person withdraws his consent to the material being held it is difficult to see how this can then be "retained until it has fulfilled the purpose for which it was taken or derived".

17. Clause 10 states that if the person who provides material voluntarily is "a person who is convicted of a recordable offence, or a person who has previously been convicted of a recordable offence (other than a person who has only one exempt conviction) the material may be retained indefinitely." Whilst the Commissioner would not seek to disagree with the indefinite retention of material in such circumstances it is confusing to find this reference in a Clause that deals with the retention of material provided voluntarily on the basis of written consent that can be withdrawn at any time. Clarification is required here in order to understand how the consent arrangements will work in practice.

18. 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.

19. 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

20. 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.

21. The Commissioner would draw the attention of Parliament to the provision in clause 26(4), which allows a child to overrule a parental decision to allow his or her biometric information to be processed. This provision may sit uneasily with established legal principles concerning competence and parental consent. Is the intention that a child of any age or degree of competence should have this right? It is worth noting that the issue of *parental* competence is dealt with at clause 27(1)(b), and it would seem unusual that the issue of the child's competence is not also considered.

22. This provision 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.

23. 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"?

24. 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

25. 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 Data Protection Act 1998 (DPA) will still apply where images related to individuals are involved 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 any confusion.

26. 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 on 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. 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.

27. 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 request to view and have copies of images of themselves.

28. 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 may be unrealistic to expect 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.

29. The Commissioner is pleased that the Bill includes the broad title of "surveillance camera systems" and refers specifically to closed circuit television and automatic number plate recognition systems. Clause 30 (6)(b) refers to "any other systems for recording or viewing visual images of objects or events for surveillance purposes". It is not clear why the reference to "objects or events" is necessary and whether this is intended to limit the scope of the code. In particular it is not clear whether this definition includes surveillance systems that view and process images of individuals. This approach contrasts with data protection law where the focus is on personal information rather than equipment. This future proofs the legislation and allows it to cover images captured by internet protocol cameras, body worn devices, cameras recording directly to digital storage media and mobile phones. It also covers data transmitted via computer networks or the internet and includes processing such as facial recognition, gait analysis and other video analytics technologies. Given the numerous sources of image capture, the Commissioner's priority is to regulate the use of the personal data rather than focus on the equipment used to capture it.

30. 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 application of the code to the police and local government only.

31. 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 needs clarifying.

32. The Information Commissioner would see great value in working closely with any future Surveillance Camera Commissioner. In order to have an effective, transparent and consistent regulatory framework, it is essential that all the commissioners who have a role in overseeing camera surveillance have clear and complementary roles. Otherwise there is a risk that regulation becomes fragmentary, confusing and contradictory, especially if commissioners take different approaches.

33. The Camera Surveillance Commissioner's functions include encouraging compliance with and reviewing the operation of the surveillance camera code. In addition, Clause 34 (2) states that the Camera Surveillance 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.

34. 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.

Part three, chapter two – vehicles left on land

35. The Information Commissioner welcomes the proposals as they will increase transparency for keepers of vehicles, but has some concerns about the consequences that the creation of the offence of immobilising vehicles will have, as private car park operators will need to seek alternative methods for enforcing the restrictions that they have put in place on the land for which they are responsible.

36. Clause 55 clearly provides this alternative route. The Commissioner welcomes the clarification that this clause provides in relation to when, and under what circumstances, a car park operator can legitimately request information from the Driver and Vehicle Licensing Agency (DVLA). The Commissioner is concerned about the increased flow of personal data that will undoubtedly result from the provisions in this Bill. In our experience, increased data flows generally mean increased data protection risks and these should be mitigated as far as possible.

37. There is a question of whether processing the registered keeper's personal data for these purposes would have difficulty in meeting the 'lawful' and 'fair' requirements of the first principle of the DPA. This relates to the difficulties that may arise in terms of the registered keeper being a third party to a contract between the driver and car park operator and being held liable for a contract that was entered into without the registered keeper's knowledge or approval.

38. Schedule 4(6) of the Bill sets out the obligations that a car park operator would need to comply with, in order to legitimately request registered keeper information from the DVLA. This will place additional demands upon the DVLA, not just in relation to the increased volume

of requests that they will undoubtedly receive but also in terms of the checks that they will need to undertake to confirm that requests are legitimate, as well as meeting the existing criteria for demonstrating 'reasonable cause', and that car park operators have met their obligations under this Bill.

39. Schedule 4(6)(2) lays out the criteria which should be included in the notice informing a driver of a parking charge. This measure will help ensure transparency in the levying of charges. These notices could be improved by including reference to the fact that liability will fall to the registered keeper of the vehicle where a driver fails to pay and the creditor is unable to identify or contact them. This will be helpful in ensuring greater transparency and fairness for drivers; it may also have a deterrent effect in terms of encouraging drivers to take responsibility for parking charges which they incur, rather than ignoring any notice that they receive.

40. Schedule 4(6)(3) stipulates that the parking charge notice should be physically handed to the driver of the vehicle or affixed to the vehicle while it is on the operators premises and stationary. The ICO has received complaints in which vehicle owners have received retrospective parking charge notices from car park operators who have used CCTV and ANPR technology to identify vehicles which have contravened their parking rules. As such this provision is welcome. This provision appears to mandate the use of notices if car park operators wish to access information from DVLA. The use of CCTV and ANPR cameras, without issuing a notice in this way, will not satisfy the criteria laid out in this Bill.

Part five - safeguarding vulnerable groups, criminal records etc

41. 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.

42. 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.

43. 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 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.

44. 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.

45. 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.

46. 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

47. 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.

48. The Commissioner welcomes Clause 71 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.

49. 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 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 then the disclosure of this information then they are then 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.

50. 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.

51. Clause 72 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 this 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

52. The Commissioner welcomes provisions in Clause 77 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. 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.

53. Clause 78 introduces provision to remove the duty of the Secretary of State to issue the relevant certificate where the applicant is aged less than 16 years. However, the Bill does not make it clear whether the Secretary of State still has a discretionary power to issue the relevant certificate where the person is less than 16 years.

54. If it is not made clear whether the Secretary of State has this discretion it may fall to the Information Commissioner to make a decision as to whether the issuing of a certificate in any given case was in compliance with the DPA. This is because on receipt of a complaint from an individual the ICO will need to decide whether the processing of personal information in order to issue a certificate was lawful. It may be difficult for the Information Commissioner to make such a decision if the extent of the Secretary of State's discretionary powers is not clear in the legislation.

55. 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 79. 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.

56. The Commissioner supports the introduction of provisions to update certificates in Clause 80. 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.

57. 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.

58. 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 81

59. The commencement of s112 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 s56 DPA as a matter of urgency. The opportunity to introduce these important and long over due measures should not be missed.

60. If s112 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.

61. 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 three - disregarding certain convictions for buggery etc.

62. 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.

63. 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.

64. Secondly, the use of the word "delete" in relation to the disregarding of offences is misleading. "Delete" should be given its ordinary meaning and should not be redefined as recording the fact the conviction or caution is disregarded and the effect of it being such a conviction or caution.

65. It is not sufficiently clear in the Bill to what "relevant official records" the definition of "delete" applies to. Does the definition of "delete" in the Bill apply only to "(b) such other official records as may be prescribed" as the definition seems to suggest or does the definition of "delete" apply to all "relevant official records" under parts (a) and (b) of this definition including "the names database". In short, will the chief police officer delete, in the ordinary meaning of the word, details of all convictions and cautions when a decision to disregard is made by the Secretary of State or will it only be subject to deletion as defined in the Bill?

Part 6 - Freedom of Information and Data Protection

66. The Commissioner welcomes the changes proposed to the 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.

67. It is important that the FOIA is updated to take account of new possibilities to promote openness using internet technologies. This has been referred to 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.

68. 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.

69. The changes to sections 11, 19 and 45 of FOIA proposed in clause 92 are positive but the Commissioner offers the following observations.

70. 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".

71. 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 if 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.

72. 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.

73. The Commissioner acknowledges that certain aspects of the changes proposed in clause 92 will become clearer when the proposed changes to the section 45 Code of Practice are published.

74. 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].

75. 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.

76. In clause 93, 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.

77. 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 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.

78. Clauses 95 to 98 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.

---

[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).

79. 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 that is not renewable. However the Commissioner draws Parliament's attention to the fact that the current term of five years was originally part of a package which included an option for the term to be renewed. 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. The Commissioner would ask Parliament to consider whether, in the light of a single fixed term and that the fact that the commissioner is a corporation sole, there might be value in increasing the length of the term for subsequent commissioners to a period of up to seven years. This would not be without precedent. For example in Canada the federal commissioner is appointed for a seven year term.

80. The measures will be underpinned by a revised Framework Document which will outline the day-to-day relationship between Government and the Information Commissioner. The Ministry of Justice has 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.