The Protection of Freedoms Bill

The Protection of Freedoms Bill deals with a wide variety of areas. It includes provisions on retention of DNA and fingerprints by the police, use of biometrics by schools, regulation of CCTV, judicial approval of surveillance, powers of entry, clamping, counter-terrorism, vetting and barring, criminal records, disregarding convictions for consensual homosexual activity, freedom of information and the Information Commissioner, trial by jury and marriage. In the course of these provisions it creates two new commissioners and requires the publication of several codes of practice.

It is, on any view, a complicated piece of legislation. A preamble to a bill is normally under a dozen words long. In this Bill it is 194 words. In addition, some of the drafting appears to have been done without full consideration, and so in places the position is incomprehensible.

This document deals with matters in the order they appear in the Bill. Each part or chapter is summarised and, in general, then followed by a detailed description of each clause.

	page
Part 1 – Regulation of Biometric Data	2
Chapter 1 – Destruction, Retention and Use of Fingerprints etc	2
Chapter 2 – Protection of Biometric Information of Children in Schools etc	8
Part 2 – Regulation of Surveillance	9
Chapter 1 – Regulation of CCTV and other Surveillance Camera Technology	9
Chapter 2 – Safeguards for Certain Surveillance under RIPA	11
Part 3 – Protection of Property from Disproportionate Enforcement Action	12
Chapter 1 – Powers of Entry	12
Chapter 2 – Vehicles Left on Land	12
Part 4 – Counter-Terrorism Powers	13
Part 5 – Safeguarding Vulnerable Groups, Criminal Records etc	14
Chapter 1 – Safeguarding of Vulnerable Groups	14
Chapter 2 – Criminal Records	14
Chapter 3 – Disregarding Certain Convictions for Buggery etc	15
Part 6 – Freedom of Information and Data Protection	16
Part 7 – Miscellaneous and General	17

Part 1 – Regulation of Biometric Data

Chapter 1 – Destruction, Retention and Use of Fingerprints etc

This chapter introduces, in Clauses 1-25, a modified version of the Scottish model of DNA and fingerprint retention. A tabular version of the Bill's proposals is provided at Annex B in the Explanatory Notes (see table below). The difficulty with this chapter is the role of the Commissioner for the Retention and Use of Biometric Material, which appears not to be clearly defined (for more information see Clauses 20 and 21). In addition, the requirements for transitional provisions appear to be undefined (see Clause 25) and the Bill treats persons who are cautioned, reprimanded or finally warned as though they were convicted (see Clause 18).

Occurrence	Current System (E&W)	Crime and Security Act 2010	Scottish System	Bill
Adult – Conviction – All Crimes	Indefinite	Indefinite	Indefinite	Indefinite
Adult – Non-conviction – Serious Crime	Indefinite (save 'exceptional circumstances')	6 years	3 years + possible 2 year extension(s) by Court	3 years + single possible 2 year extension by Court
Adult – Non-conviction – Minor Crime	Indefinite (save 'exceptional circumstances')	6 years	None	None (speculative search possible)
Under 18 – Conviction – Serious Crime	Indefinite (save 'exceptional circumstances')	Indefinite	Indefinite	Indefinite
Under 18 – Conviction – Minor Crime	Indefinite (save 'exceptional circumstances')	1st conviction – 5 years; 2nd - indefinite	Indefinite	1st conviction – 5 years (plus length of any custodial sentence); 2nd conviction - indefinite
Under 18 – Non-conviction – Serious Crime	Indefinite (save 'exceptional circumstances')	3 years	3 years +possible 2 year extension(s) by Court	3 years + single possible 2 year extension by Court
Under 18 – Non-conviction – Minor Crime	Indefinite (save 'exceptional circumstances')	3 years	None	None (speculative search possible)
Terrorist suspects	Indefinite (save 'exceptional circumstances')	6 years + renewable 2 year period(s) on national security grounds	Not covered (reserved matters)	3 years + renewable 2 year period(s) on national security grounds
Biological DNA Samples	Indefinite (save 'exceptional circumstances')	Within six months of sample being taken	As per destruction of profiles	Within six months of sample being taken

Three short definitions are necessary before discussing clauses:

- **Recordable offences** are set out in the National Police Records (Recordable Offences) Regulations 2000. Almost every offence is recordable, as the term includes any offence punishable by imprisonment.

- A **qualifying offence** is defined by section 65A of the Police and Criminal Evidence Act 1984 (inserted by section 7 of the Crime and Security Act 2010). It includes the most serious offences (murder, kidnap and so on), but also extends to assault occasioning actual bodily harm, burglary. It would also include consensual sexual activity between young people under 16.

- An **excluded offence** is defined by Clause 3 of the Bill. It means any offence which is not a qualifying offence, is the only offence of which the person has been convicted, was committed when the person was aged under 18 and for which they were not sentenced to 5 years or more in custody.

Clause 1 regulates the circumstances in which the police may retain fingerprints and DNA profiles (referred to in the Bill as 'section 63D material', but in this briefing as 'material'). Material must be destroyed if it appears to the relevant chief officer of police that the material was taken unlawfully, that the person was arrested unlawfully or that their arrest was based on mistaken identity. In other circumstances material must be destroyed, unless a subsequent power permits it to be retained.

Clause 2 provides that material can be retained until the conclusion of an investigation into an offence or of related proceedings.

Clause 3 applies to material which relates to a person who was arrested for or charged with a qualifying offence, but is not convicted of that offence; and which was taken in connection with the investigation of the offence. Material can be retained indefinitely under this clause, if:

- the person has previously been convicted of a recordable offence (which is not an excluded offence); or
- the person is convicted of a recordable offence (which is not an excluded offence) before the material is required to be destroyed.

Otherwise, material may be retained for a specified retention period if:

- it relates to a person who is charged with a qualifying offence, but is not convicted of that offence and was taken in connection with the investigation of that offence; or
- it relates to a person who is arrested for a qualifying offence, but is not

charged with that offence, it was taken in connection with the investigation of the offence and any prescribed circumstances apply.

The retention period is 3 years (which, in the case of DNA material, begins to run from the day on which the sample was taken). This may be extended by an order of a District Judge (Magistrates' Courts), acting on the application of a chief officer of police made within the last 3 months of the retention period. This order may extend the retention period by up to 2 years. The District Judge's order, or refusal to make an order, may be appealed to the Crown Court by a chief officer of police or the person from whom the material was taken.

'Prescribed circumstances' means circumstances prescribed in a statutory instrument by the Secretary of State. A draft of the instrument must be placed before both Houses of Parliament. The circumstances prescribed must include the fact that the Commissioner for the Retention and Use of Biometric Material has consented to the retention of the material concerned. They may also include the procedure for decisions by, and appeals from, the Commissioner. This provision seems odd, as the Commissioner (discussed in relation to clause 20 below) appears to have no powers outside the area of national security.

Clause 4 applies to material taken in connection with an investigation which relates to a person who is arrested for or charged with a recordable (but non-qualifying) offence or offences, and is not convicted. If the person has previously been convicted of a recordable (but not excluded) offence, the material may be retained indefinitely.

Clause 5 provides that if a person is convicted of a recordable offence, any material taken in connection with the investigation may be retained indefinitely.

Clause 6 provides that if a person has been required to supply material because they were convicted of an offence outside England and Wales which, if committed inside, would amount to a qualifying offence, then the material may be retained indefinitely.

Clause 7 provides that if a person is convicted of a recordable non-qualifying offence which they committed while under 18, and have not previously been convicted of a recordable offence, then material taken in connection with the investigation of the offence can be retained:

- if sentenced to five years or more in custody, indefinitely;
- if sentenced to less than five years in custody, five years after the end of the sentence;
- if not sentenced to custody, five years from the date on which the fingerprints or DNA sample was taken.

Clause 8 provides that material which relates to a person who was given a fixed penalty notice, and was taken from them in connection with the investigation of

the offence, may be retained for a period of two years from the fingerprints or sample being taken.

Clause 9 provides that material may be retained for as long as a chief officer of police determines that it is necessary for the purposes of national security. This determination must be made in writing and has effect for a renewable period of two years at a time.

Clause 10 provides that material given voluntarily may be retained until it has fulfilled the purpose for which it was taken, and if it relates to a person who is, or has previously been, convicted of a recordable offence (other than one exempt conviction) it may be retained indefinitely.

Clause 11 applies to material which relates to a person who consents to its retention. The material may be retained for as long as the person consents. Consent must be in writing, and can be withdrawn at any time. It is not clear if the withdrawal of consent must also be done in writing.

Clause 12 provides that material taken in connection with the investigation of one offence is to be (if the investigations leads to the person being arrested for, charged with or convicted of another offence) treated as though it were taken in connection with the latter offence.

Clause 13 provides that if fingerprints are required to be destroyed, any copies of them must also be destroyed. If a DNA profile is required to be destroyed, no copy may be retained except in a form which does not include information which identifies the person to whom it relates. The purpose of this provision is unclear, as the purposes set out in Clause 16 seem not to be capable of being carried out through the use of anonymised data.

Clause 14 applies to samples taken from a person under compulsory powers, or taken with consent in connection with the investigation of an offence. These samples must be destroyed it appears to a chief officer of police that it was taken unlawfully or because of an arrest which was unlawful or based on mistaken identity. Any other DNA sample must be destroyed as soon as a DNA profile has been derived from it or, if sooner, within 6 months of it being taken. Any other sample must be destroyed within 6 months. A speculative search in relation to the samples may be carried out within a reasonable time if a chief officer of police considers it to be desirable.

Clause 15 applies to impressions of footwear taken under compulsory powers or with consent. It provides that they may be retained for as long as is necessary for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution, but must otherwise be destroyed.

Clause 16 provides that any material, sample or impression of footwear must not be used other than:

- in the interests of national security;
- for a terrorist investigation;
- for the prevention or detection of crime;
- for the investigation of an offence (whether inside or outside England and Wales);
- for the conduct of a prosecution (whether inside or outside England and Wales);
- for the identification of a deceased person; or
- for the identification of the person to whom the material relates.

'Used' includes allowing any check to be made against the material and disclosing it to any person. 'Crime' includes any conduct which is a criminal offence under the law of England and Wales or of any other country. This is potentially a very broad provision.

Material which is required to be destroyed must not, after that time, be used in evidence against the person or for the investigation of any offence.

Clause 17 provides that these clauses do not apply to material related to terrorism or immigration controls.

Clause 18 sets out various definitions. In particular, it provides that 'conviction' includes cautions, reprimands or final warnings. It should be noted that reprimands and final warnings, which are the equivalent of cautions for young people, can be imposed without their consent.

Clause 19 repeals various pieces of legislation, as set out in Schedule 1 to the Bill.

Clause 20 provides that the Secretary of State must appoint a Commissioner for the Retention and Use of Biometric Material ('the Biometrics Commissioner'). The function of this Commissioner is to review every national security determination made under Clause 9, or under various pieces of terrorism legislation, as well as the uses to which material retained for national security reasons is put. Every person who makes or renews a national security determination must supply a copy of the determination to the Biometrics Commissioner, as well as any documents or information the Biometrics Commissioner requires. The Biometrics Commissioner may order the destruction of material if it is not necessary for national security and it is not otherwise capable of being lawfully retained. The Biometrics Commissioner's budget is to be determined by the Secretary of State, who may also provide the Biometrics Commissioner with such staff, accommodation, equipment and other facilities as the Secretary of State considers necessary.

Clause 21 provides that the Biometrics Commissioner must make annual reports, and may make further reports at any time. The Secretary of State may

require the Biometrics Commissioner to report on any matter relating to the retention of biometric material by a law enforcement authority for the purposes of national security. Any report must be published and laid before Parliament, although the Secretary of State may exclude any part which, if published, would be contrary to the public interest or prejudicial to national security.

It is clear from these clauses that the Biometrics Commissioner's role is in relation to national security. All of its functions relate to national security, as do its reports. The Biometrics Commissioner's title, therefore, seems rather broader than its actual remit. Its inclusion in Clause 3 seems, given the lack of any relevant power, to be an error.

Clause 22 mandates the Secretary of State to give guidance about making or renewing national security determinations, and permits her to give guidance for other purposes.

Clause 23 provides that any DNA profile which is retained under Clauses 4-8 must be recorded on the National DNA Database.

Clause 24 provides that the Secretary of State must create a National DNA Database Strategy Board. The Board will oversee the Database's operation and issue guidance about the destruction of profiles (which chief officers of police must comply with). The Secretary of State must publish the governance rules of the Board. The Board must make an annual report about the exercise of its functions. The Secretary of State must publish this report, although she may exclude any part which it would be contrary to the public interest or prejudicial to national security to publish.

Clause 25 deals with material taken before the Bill's commencement.

The Secretary of State must, by statutory instrument on the negative resolution procedure, provide for the destruction or retention of such material. These provisions must ensure that, in the cases of persons arrested for or charged with, but not convicted of an offence, that:

- where it is a qualifying offence committed more than 3 years before the commencement day, the material is destroyed;
- where it is a qualifying offence committed less than 3 years before the commencement day, the material is destroyed within 3 years;
- where it is not a qualifying offence, the material is destroyed.

Sub-clause (4) appears to undermine this position, however, as it states that an order may provide for exceptions to it. In the circumstances, this seems to render the detailed provision pointless.

Chapter 2 – Protection of Biometric Information of Children in Schools etc

These provisions, in Clauses 26-28, apply to educational institutions for under-18s. They require consent of both parents and the child before any processing of biometric information takes place. The information cannot be processed if the child objects at any time, or if either parent withdraws their consent in writing. This Chapter, however, does not define 'biometric' with sufficient precision (see Clause 28).

Clause 26 applies to schools, 16-19 Academies or further education institutions. It provides that, in order to process the biometric information of a child (under 18), either both parents of the child must have consented to the information being processed or one of the exceptions to consent must apply. However, the authority must not process the information if at any time the child refuses to participate, continue to participate, or otherwise objects to its processing. The authority must have reasonable alternative means of doing anything that would normally involve the processing of biometric information. While it seems clear that this is the effect of the Clause, amendment will be necessary to improve the quality of the drafting.

Clause 27 provides that a parent's consent is not required if the authority is satisfied that:

- the parent cannot be found;
- the parent lacks capacity;
- the welfare of the child requires that the parent is not contacted;
- it is otherwise not reasonably practicable to obtain the parent's consent.

Where consent is obtained it can be withdrawn at any time. It must be given and withdrawn in writing. These provisions are in addition to the requirements of the Data Protection Act 1998.

Clause 28 sets out various definitions. It defines biometric information as being information about a person's physical or behavioural characteristics or features which is capable of being used to identify the person and is obtained for the purpose of being so used. It may, in particular, include information about the skin pattern and other characteristics of a person's fingers or palms, information about the features of an iris or other part of they eye and information about a person's voice or handwriting.

However, it may be that this definition is not sufficient to cover all cases. It is commonly thought that the information which authorities possess is not capable of being re-converted into, for example, a fingerprint. Given that belief, it may that a school would seek to argue that the information they hold is not information about a person's physical characteristics. Without wishing to discuss the merits of a view, it may be that a definition of biometric information as

'information about or derived from a person's physical or behavioural characteristics or features' would avoid any doubt.

Part 2 – Regulation of Surveillance

Chapter 1 – Regulation of CCTV and other Surveillance Camera Technology

This Chapter requires the Secretary of State to produce a code of practice in relation to surveillance cameras. There is provision for it to cover a range of issues, from technical specifications to the processing of the information they gather. Clauses 34 and 35 govern the appointment and powers of a new Surveillance Camera Commissioner.

Clause 29 provides that the Secretary of State must prepare a code of practice containing guidelines about surveillance camera systems. The code must cover either the development or use of such systems, or the use or processing of images and information obtained by them, or both. The code may also cover:

- considerations about whether to use surveillance camera systems;
- the types of such systems;
- technical standards applicable to them;
- appropriate locations for them;
- publication of information about them;
- standards applicable to persons using or maintaining surveillance camera systems;
- standards applicable to persons using or processing information obtained by virtue of such systems;
- access to or disclosure of information so obtained;
- procedures for complaints or consultation.

However, the code need not contain guidance about every type of surveillance camera. This provision is intended to avoid the need for the code to cover niche or developing systems, but it may lead to lacunae. Guidance about different types of system need not be identical. In the course of preparing this code of practice, the Secretary of State must consult with:

- persons who are likely to be subject to a duty to follow the code;
- ACPO;
- the Information Commissioner;
- the Chief Surveillance Commissioner;
- the Surveillance Camera Commissioner;
- the Welsh Ministers;
- any other person the Secretary of State feels appropriate.

'Surveillance camera systems' includes CCTV and automatic number plate recognition systems (ANPR), as well as any other system that records, stores,

receives, transmits or processes this data or any other images if they are for 'surveillance purposes'.

Clause 30 sets out the procedure by which the code of practice must be issued. The code must be approved by both Houses of Parliament. If the code is not approved, and the Secretary of State considers there is no realistic prospect of this happening, the Secretary of State must prepare another code of practice.

Clause 31 provides that the Secretary of State must keep the code under review, and may prepare alterations or a replacement code. Before doing this, the same people must be consulted as were required in clause 29. The replacement code must then be laid before Parliament and will be issued in 40 days, unless a resolution not to approve it is passed by either House. The 40-day period begins with the day (or the latest day, if laid before each House separately) on which the code is laid before Parliament. Days on which Parliament is dissolved or prorogued do not count towards the 40 days.

Clause 32 requires the Secretary of State to publish the code of practice and any replacement codes or alterations that are issued.

Clause 33 provides that a 'relevant authority' that exercises functions to which the code relates must have regard to the code when exercising them. However, a failure to have regard to the code does not of itself give rise to any liability to criminal or civil proceedings. The code will be admissible in any criminal or civil proceedings. The court or tribunal in such proceedings will, in making its decisions, be able to take into account failures to have regard to the code.

A 'relevant authority' includes:

- local authorities;
- police and crime commissioners;
- chief officers of police forces in England and Wales;
- any person specified by the Secretary of State in an order.

An order can contain a description that is restricted to a person acting only in a specified capacity, or when exercising specific functions. Before making such an order the same people as referred to in clause 29 must be consulted, as well as the person to be affected by it. Such an order can only be made after approval by both Houses.

Clause 34 provides that the Secretary of State must appoint a Surveillance Camera Commissioner (SCC). The SCC's functions will be to encourage compliance with the code of practice, to review the operation of the code and to provide advice about the code, including about any changes or breaches of it. The Secretary of State may pay expenses, remunerations or allowances in respect of the SCC, and provide the SCC with such staff, accommodation,

equipment or other facilities as the Secretary of State feels necessary for the SCC to carry out its functions.

The SCC does not appear to have any regulatory or enforcement function.

Clause 35 provides that the SCC must prepare an annual report as soon as reasonably practicable after the end of each 'reporting period' on the exercise of its functions. The Secretary of State must be given a copy that must be laid before Parliament, and the SCC must publish it.

Chapter 2 – Safeguards for Certain Surveillance under RIPA

Under RIPA (Regulation of Investigatory Powers Act 2000), communications data can be obtained if certain conduct is authorised or a notice is given for it to be disclosed. The types of conduct that can be authorised include directed surveillance (which must not be intrusive, for example by having an individual or a surveillance device in any residential premises) and use of covert human intelligence sources (CHIS). Authorisations and notices can only be given if:

- it is believed to be necessary to obtain the data, under grounds such as national security, public safety, or other purposes specified in an order by the Secretary of State; and
- it is believed that the conduct authorised or required to obtain it is proportionate to what is sought to be achieved once it is obtained.

Authorisations or notices can only be given by a 'designated person'. Currently, such persons are designated in the Regulation of Investigatory Powers (Communications Data) Order 2010/480, and are generally police officers above superintendent rank or departmental managers in enforcement agencies.

This Chapter of the Bill inserts new sections into RIPA that require additional judicial approval by (in England and Wales) a magistrate before the authorisation or notice can take effect.

Clause 37 inserts sections 23A and 23B into RIPA. At present, section 23 of RIPA governs authorisations and notices for obtaining and disclosing communications data obtained by postal and telecommunications services. New section 23A will require judicial approval to be given before any authorisation is effective, and so before any interception can take place. Approval may be given only if the magistrate is satisfied that:

- at the time the authorisation or notice was granted or renewed, there were reasonable grounds to believe it was necessary and proportionate to do so (as outlined in the two bullet points above); and
- at the time the magistrate is considering the matter, there are still reasonable grounds to hold those beliefs.

The magistrate must also be satisfied that the individual giving the authorisation or notice was in fact a 'designated person'. There is also provision that the Secretary of State may by order set further conditions to be satisfied, subject to the negative resolution procedure of both Houses of Parliament.

New section 23B sets out the procedure for obtaining judicial approval. The public authority to which the designated person belongs can apply for approval of the authorisation or notice they have given. They do not have to inform any person to whom the notice or authorisation relates, or that person's legal representatives. If approval is not given, the magistrate may make an order quashing the authorisation or notice.

Clause 38 inserts section 32A and 32B into RIPA. Section 32 of RIPA relates to the authorisation of directed surveillance and the use of CHIS. The new sections require judicial approval of these authorisations before they can take effect. The conditions to be satisfied and the procedure are essentially the same as those in sections 23A and 23B as outlined above.

Under section 43 of RIPA there is an additional review that must be carried out when renewing authorisations for use of CHIS. Clause 38 provides that the magistrate must be satisfied that the review was carried out, and consider the results of the review themselves, before granting judicial approval.

Part 3 – Protection of Property from Disproportionate Enforcement Action

Chapter 1 – Powers of Entry

This Chapter contains various provisions relating to the repeal, rewriting and review of powers of entry onto land. It also gives national authorities the power to add safeguards to these powers. Clauses 47-52 provide for a code of practice for non-devolved powers of entry to be written and maintained by the Secretary of State.

Chapter 2 – Vehicles Left on Land

Clause 54 sets out provisions relating to using immobilising devices or restricting the movement of vehicles, and creates an offence for unlawfully doing so. This clause is primarily intended to deal with issues that have arisen recently in relation to car clamping.

Clause 55 extends the current powers to remove vehicles left on roads (for example, if abandoned or dangerously parked) to vehicles also left on land other than roads.

Clause 56 brings Schedule 4 of the Bill into effect, which governs the procedure for recovery of unpaid parking charges.

Part 4 – Counter-Terrorism Powers

Clauses 57-62 reduce the maximum period for which terrorism suspects can be detained and places some limits on the circumstances in which police officers may search individuals without reasonable suspicion.

Clause 57 reduces the maximum period that individuals suspected of terrorism offences can be detained in police custody from 28 to 14 days.

Clause 58 repeals the stop and search powers contained in sections 44-47 of the Terrorism Act 2000.

Clause 59 amends section 43 of the 2000 Act, which deals with searches made of people who a police officer reasonably suspects to be terrorists. It removes the requirement that a search be conducted by an officer of the same sex. In addition, it provides that if a search is conducted of a person in a vehicle, the officer may search the vehicle and retain any item which they reasonably suspect may constitute evidence that the person is a terrorist.

Clause 59 also inserts a new section 43A to the 2000 Act, which provides that a police officer may stop and search a vehicle, its driver and passengers if they reasonably suspect that the vehicle is being used for the purposes of terrorism.

Clause 60 provides that an officer of at least the rank of Assistant Chief Constable (or Commander, in London) may give an authorisation in relation to a specified area or place if they reasonably suspect that an act of terrorism will take place and consider that the authorisation is necessary to prevent such an act, and that its duration and extent are no greater than necessary. In an area covered by an authorisation a uniformed police officer may stop and search any person or vehicle without reasonable suspicion. However, this power may only be exercised for the purpose of discovering evidence of terrorism. Schedule 5 contains various supplementary provisions.

Clause 61 provides that the Secretary of State must prepare, and lay before Parliament for approval, a code of practice on the use of these powers. A police officer must have regard to this code, although breach of it does not, of itself, make them liable to civil or criminal proceedings.

Clause 62 gives effect to Schedule 6, which amends stop and search procedures in Northern Ireland.

Part 5 – Safeguarding Vulnerable Groups, Criminal Records etc

Chapter 1 – Safeguarding of Vulnerable Groups

Clauses 63-76 amend the Safeguarding Vulnerable Groups Act 2006. These clauses appear to reduce the scope of the barring scheme. They reduce the scope of activities from which individuals are barred in relation to both children and vulnerable adults, require an indication that a person may engage in relevant work before they can be barred and abolish the requirement for monitoring of individuals seeking to work with children or vulnerable adults. A detailed summary of these provisions is provided in the Explanatory Notes between paragraphs 256-293.

Chapter 2 – Criminal Records

This Chapter, in clauses 77-81 amends the Police Act 1997. The amendments only deal with the sections related to criminal record certificates (sometimes known as CRB certificates). There are two types of certificate:

- A regular **certificate**, which contains information about the individual's previous convictions and cautions; and

- An **enhanced certificate**, which may also contain 'soft intelligence'.

The amendments in this Bill add safeguards to the process of obtaining a certificate, and make changes to the content of such certificates.

Clause 77 repeals the requirement for copies of the certificate to be sent to the registered person. The current state of the law is that an application for a certificate must be countersigned or electronically sent by a registered person to the Secretary of State. Once the application is processed, a certificate will be sent to the individual to whom it relates, with a copy sent to the registered person, who must be:

- an incorporated or unincorporated body;
- a person appointed to an office; or
- an individual who employs others in a business.

In most cases this will be a potential employer with whom the individual is applying for a job. This repeal means that a copy will no longer be sent to them, giving individuals a chance to challenge the information on the certificate without it having been revealed to the employer already. It appears that it will be the responsibility of the individual to pass the certificate on to the employer if they do not wish to challenge it.

Clause 78 provides that an individual cannot apply for a certificate unless they are aged 16 or over. It also provides that a person cannot apply to become a registered person (as described above) unless they are aged 18 or over.

Clause 79 amends the test to be applied by a chief officer when deciding what non-conviction information to provide to the Secretary of State for the creation of an enhanced certificate. The test used to be that any information that the officer was of the opinion 'might be relevant' and 'ought to be included' should be provided. The new test replaces the word 'might' so that the officer must now 'reasonably believe' the information to be relevant. This imposes a slightly higher test.

The clause will add a requirement that any officer making the decision described above must also have regard to any guidance published by the Secretary of State.

This clause also amends what is required of the Secretary of State. Currently, to gather information for an enhanced certificate, the chief officer in every relevant police force must be contacted. The amended provision will require only that one of the relevant officers be contacted. It is intended that this single officer (or a group of officers from a small area) could make all decisions relating to non-conviction information held by all police forces.

This clause also expands the provisions for requesting a review of the contents of a certificate. The Secretary of State will be required to ask the relevant chief police officers to review the relevancy of the information they provided for enhanced certificates.

Clause 80 provides for a new procedure by which certificates can be up-dated. An applicant can only subscribe to the up-date service at the same time as applying for a new certificate. The subscription will need to be renewed on an annual basis. A subscriber to the up-date service can make a request for up-date information to the Secretary of State. This means that they will be told either:

- that there is no new conviction information (or other information in the case of enhanced certificates) that would be included on a new certificate; or
- that they are advised to apply for a new certificate (meaning that new information now exists).

Clause 81 provides that a criminal record certificate must include information about any conditional cautions the individual has, as well as convictions.

Chapter 3 – Disregarding Certain Convictions for Buggery etc

Clauses 82-91 create a scheme under which convictions for consensual homosexual activity between adults can be removed from individuals' criminal records. The Secretary of State will consider applications and, if it appears that both parties were consenting and aged over 16, notify controllers of relevant

databases to disregard the conviction. The individual may appeal to the High Court if their application is rejected by the Secretary of State.

If a conviction is disregarded the individual will be treated as those they had not committed any offence. No evidence of their conviction will be admissible before any court, and they will not have to disclose it if asked.

Part 6 – Freedom of Information and Data Protection

Clauses 92-98 provide for greater disclosure of datasets from public authorities, and provide a slight increase in the powers of the Information Commissioner, who no longer requires the consent of the Secretary of State to some guidance and for staffing levels.

Clause 92 requires public authorities to disclose datasets in re-usable form. It provides that where a freedom of information request is made for information in a dataset and the person making the request asks for it to be supplied in electronic form, the public authority must, so far as is reasonably practicable, supply the information in an electronic form which is capable of re-use. A dataset means a collection of information, held in electronic form, that has been obtained or recorded to provide a public authority with information about the carrying out of their services or functions. The information in it must be factual, rather than analysis or interpretation.

Clause 92 also provides that where the public authority is the only copyright owner, they must make the dataset available on the basis of a licence which the Secretary of State will set out in guidance. Public Authority publication schemes must also include any dataset they hold which has been requested, including any updated version of it, unless it is not appropriate to publish it.

Clause 93 amends the Freedom of Information Act 2000 to include wholly-owned government companies where the company's ownership is divided between government departments, the Crown or other public bodies. It changes the definition of 'wholly-owned', in a manner which the Explanatory Notes suggest will include waste disposal companies and purchasing organisations owned by a number of local authorities.

Clause 94 will place Northern Ireland on the same footing as the rest of the UK in the application of the exemption of information which contains communications with the Royal Family and Household.

Clause 95 amends Schedule 5 of the Data Protection Act 1998, which deals with the appointment and removal of the Information Commissioner. It provides that no Parliamentary motion for his dismissal may be proposed unless a Minister of the Crown has presented a report stating that they are satisfied that the Information Commissioner:

- has failed to discharge the functions of the office for at least 3 months;
- has failed to comply with the terms of appointment;
- has been convicted of a criminal offence;
- is an undischarged bankrupt;
- has made an arrangement or composition contract with, or has granted a trust deed for, the Commissioner's creditors; or
- is otherwise unfit to hold the office or unable to carry out its functions.

The Clause also provides that no person may be appointed unless they have been selected on merit on the basis of fair and open competition, and that the Information Commissioner may not be appointed for a further term of office.

Clause 96 provides that the Information Commissioner must consult the Secretary of State before issuing, altering or replacing codes of practice on assessment notices, data-sharing and monetary penalty notices. This replaces provisions which required the Secretary of State's approval for any code.

Clause 97 provides that the Information Commissioner may, without needing to obtain the Secretary of State's consent, charge for providing training, conferences or providing more than one copy of any published material. The Secretary of State may, by order, amend this list.

Clause 98 provides that the Information Commissioner does not require the approval of the Secretary of State for the number and conditions of his staff. It also provides that, in making appointments, the Information Commissioner must have regard to the principle of selection on merit on the basis of fair and open competition.

Part 7 – Miscellaneous and General

Clause 99 repeals the section of the Criminal Justice Act 2003 that permits certain fraud cases to be conducted without a jury.

Clause 100 allows (and repeals the offence of officiating) marriages and registrations of civil partnerships outside the hours of 8am and 6pm.

Conclusion

If we can be of any further assistance, please contact us at alex@dubio.co.uk or hayley.boot@dubio.co.uk. We are happy to write more detailed explanations of any of the Bill's clauses, or to assist with other documents including second reading briefings or amendments. This document is available through our Twitter feed, CSAdviceGroup.

Alex Dowty
Hayley Boot

22nd February 2011