ILPA information for debate on NC 15 Suppy of Information to the Secretayr of State

Immigration Act 1999

20.— Supply of information to Secretary of State.

(1) This section applies to information held by—

(a) a chief officer of police;

(b) the National Crime Agency 1

(d) […]

(e) a person with whom the Secretary of State has made a contract or other arrangements under section 95 or 98 or a sub-contractor of such a person; or

(f) any specified person, for purposes specified in relation to that person.

(1A) This section also applies to a document or article which—

(a) comes into the possession of a person listed in subsection (1) or someone acting on his behalf, or

(b) is discovered by a person listed in subsection (1) or someone acting on his behalf.

(2) The information, document or article may be supplied to the Secretary of State for use for immigration purposes.

(2A) The Secretary of State may—

(a) retain for immigration purposes a document or article supplied to him under subsection (2), and

(b) dispose of a document or article supplied to him under subsection (2) in such manner as he thinks appropriate (and the reference to use in subsection (2) includes a reference to disposal).

(3) "Immigration purposes" means any of the following—

(a) the administration of immigration control under the Immigration Acts;

(b) the prevention, detection, investigation or prosecution of criminal offences under those

Acts;

(c) the imposition of penalties or charges under Part II;

(d) the provision of support for asylum-seekers and their dependants under Part VI;

(e) such other purposes as may be specified.

(4) "Chief officer of police" means—

(a) the chief officer of police for a police area in England and Wales;

(b) the chief constable of the Police Service of Scotland;

(c) the Chief Constable of the Royal Ulster Constabulary.

(5) "Specified" means specified in an order made by the Secretary of State.

(6) This section does not limit the circumstances in which information documents or articles may be supplied apart from this section.

Notes

- Information sharing powers are already vast.
- They are in addition to powers of search, seizure and retention when there is any suspicion of wrongdoing.
- They are in addition to specific powers, for example the powers of information sharing with registrars under the 2014 Act and the powers under that Act to take and store biometric information.
- They are also in addition to the wide duties to share information imposed by s 26 of the Immigration, Asylum and Nationality Act 2006 (reproduced below)
- They extend to powers to share information beyond the European Union (see e.g. sources at 2)
- UK Visas and Immigration is a member of CIFAS .CIFAS members include financial services, telecoms and utility companies, including all of the high street banks and building societies. CIFAS allows its members to exchange details of applications for products or services which are considered to be fraudulent. The data may be held outside the jurisdiction and may be accessed by persons who are outside the jurisdiction. Some of the companies may be incorporated in countries other than the UK.
- The extent of the powers raises concerns over the right to respect for home and correspondence guaranteed by Article 8 of the European Convention on Human Rights and the right to respect for property guaranteed in article 1 of Protocol 1 to that Convention.
-

Sources

1. Immigration Directorate Instructions on information sharing:

https://www.gov.uk/government/collections/chapter-24-disclosure-of-information-immigration-directorate-instructions

See especially *24(3).*

2. Powers to share information with other countries of the five countries conference

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/257229/pia.pdf

Where does information shared with the Secretary of state go?

A. See Immigration, Asylum and Nationality Act 2006

36 Duty to share information
(1) This section applies to–
(a) designated customs officials,
(aa) immigration officers,

(ab) the Secretary of State in so far as the Secretary of State has general customs functions,

(ac) the Secretary of State in so far as the Secretary of State has functions relating to immigration, asylum or nationality,

(ad) the Director of Border Revenue and any person exercising functions of the Director, 1

(b) a chief officer of police, and

(c) Her Majesty's Revenue and Customs.

(2) The persons specified in subsection (1) shall share information to which subsection (4) applies and which is obtained or held by them in the course of their functions to the extent that the information is likely to be of use for–

(a) immigration purposes,

(b) police purposes, or

(c) Revenue and Customs purposes.

(3) But a chief officer of police in Scotland shall share information under subsection (2) only to the extent that it is likely to be of use for–

(b) police purposes, in so far as they are or relate to reserved matters within the meaning

of the Scotland Act 1998, or

(c) Revenue and Customs purposes other than the prosecution of crime.

(4) This subsection applies to information which–

(a) is obtained or held in the exercise of a power specified by the Secretary of State and the Treasury jointly by order and relates to–

(i) passengers on a ship or aircraft,

(ii) crew of a ship or aircraft,

(iii) freight on a ship or aircraft, or

(iv) flights or voyages, or

(b) relates to such other matters in respect of travel or freight as the Secretary of State and the Treasury may jointly specify by order.

(5) The Secretary of State and the Treasury may make an order under subsection (4) which has the

effect of requiring information to be shared only if satisfied that–

(a) the sharing is likely to be of use for–

(i) immigration purposes,

(ii) police purposes, or

(iii) Revenue and Customs purposes, and

(b) the nature of the information is such that there are likely to be circumstances in which it can be shared under subsection (2) without breaching Convention rights (within the meaning of the Human Rights Act 1998 (c. 42)).

(6) Information shared in accordance with subsection (2)–

(a) shall be made available to each of the persons or descriptions of persons specified in subsection (1), and

(b) may be used for immigration purposes, police purposes or Revenue and Customs purposes (regardless of its source).

(7) An order under subsection (4) may not specify–

(a) a power of Her Majesty's Revenue and Customs if or in so far as it relates to a matter to which section 7 of the Commissioners for Revenue and Customs Act 2005 (c. 11) (former Inland Revenue matters) applies, or

(b) a matter to which that section applies.

(8) An order under subsection (4)–

(a) shall be made by statutory instrument, and
(b) may not be made unless a draft has been laid before and approved by resolution of each House of Parliament.
(9) In this section–
"chief officer of police" means–
(a) in England and Wales, the chief officer of police for a police area specified in section 1 of the Police Act 1996 (c. 16),
(b) in Scotland, the chief constable of [the Police Service of Scotland] 3 , and
(c) in Northern Ireland, the chief constable of the Poli***ce Service of Northern Ireland,***
"designated customs official" and "general customs function" have the meanings given by Part 1 of the Borders, Citizenship and Immigration Act 2009,
"immigration purposes"has the meaning given by section 20(3) of the Immigration and Asylum Act 1999 (c. 33) (disclosure to Secretary of State),
"police purposes" has the meaning given by section 21(3) of that Act (disclosure by Secretary of State), and "Revenue and Customs purposes" means those functions of Her Majesty's Revenue and Customs specified in section 21(6) of that Act.
(10) This section has effect despite any restriction on ***on the purposes for which information may be disclosed or used.***

Section 36(2) imposes a duty to share information for immigration purposes, as defined in s.20 and 21 of the Immigration and Asylum Act 1999.

The Minister of State was questioned about the reference to "other matters" in s.36(4)(b). He replied:

> "*The agencies clearly hold intelligence information related to freight and travel that is not obtained under the powers specified in clause 31(4)(a)—the substantial part of the subsection—and which may be useful for the purposes of another agency or agencies….information gathered under entirely different legal auspices outside the Bill's scope. It would prevent any of the agencies sharing those data with other agencies…'Other matters' does not refer generically to every other matter that anyone could possibly imagine. It means, as I understand it, other matters germane to the existent and statutory base of each and every one of those agencies"* (Tony McNulty MP, Standing Committee E, 5th Session, 25 10 06, Col.208)

Section 37 Information Sharing: Codes of Practice makes provision for the Secretary of State and the Treasury jointly to issue a Code of Practice on data sharing and use under s.36. 2006 code can be read at http://www.statewatch.org/news/2008/may/uk-cop-data-share-borders.pdf

Section38 Disclosure of Information for security purposes supplements the 36 duties with powers to share information. It empowers the Secretary of State or a Chief Officer of Police to share information with the Director General of the Security Service, the Chief of the Secret Intelligence Service and the Director of GHQ to the extent that the information is likely to be of use for a purpose specified in s.1 of the Security Service Act 1989 and s.1 or s.3 of the Intelligence Services Act 1994 (namely, national security, economic well being of the UK and support in combating serious crime).. The information that can be shared is to be specified in an

order made by the Secretary of State and the Treasury. Section 38(8) provides "This section has effect despite any restriction on the purposes for which information may be disclosed or used".

As originally drafted, the clause made provision for a two-way transfer of data. It was amended however because the government realised that this was not necessary; existing powers in the Security Service Act 1989 and the Intelligence Services Act 1994, enable the security agencies listed to disclose data to the border agencies listed.

The Minister of State was questioned on why while sections 32, 33 and 36 limited the order-making powers by reference to the Secretary of State being satisfied that "there are likely to be circumstances in which it can be shared…without breaching Convention rights", this section contains no such limitation. He said:

> "I repeat that anything in the Bill, not least in clause 34 will be implemented…entirely in accordance with the UK's obligations under the 1951 convention, not to mention the 1951 European convention on human rights". (Standing Committee E, Fifth Session, 25 10, 05, col. 219)

Section 39: Disclosure to Law Enforcement Agencies gives chief officers of police power to disclose information obtained under sections 32 and 33 with police forces in the Channel Islands and the Isle of Man and with "foreign law enforcement agencies". The latter are described as "a person outside the United Kingdom with functions similar to functions of a police force in the United Kingdom or the Serious Organised Crime agency". Police forces have a range of functions and the ambit of the comparative definition is unclear.

When concerns were expressed at the apparent breadth of the provision, the Baroness Ashton of Upholland reminded peers of obligations under existing data protection legislation (see Hansard HL Report 17 01 06 GC 210ff), as had the Minister of State before her in Standing Committee E (see Standing Committee E 21 10 05, Col 219). **She** acknowledged, data protection legislation contains wide exemptions (Ibid. 17 01 06 GC210ff). She said:

> "We would have to ensure that there is a legitimate aim under Article 8(2) [of the ECHR]; that disclosure is in accordance with the law; and that any interference is proportionate to the legitimate aim." (Hansard HL Report 17 01 06 Col GC211)

In **sections** 32 and 33**, which provide** for the gathering of the information to be shared express reference is made to disclosures being in accordance with the European Convention on Human Rights, but there is no similar provision here. The Baroness Ashton of Upholland said: "we will expect chief police officers to fulfil their obligations properly" (ibid). In clauses 32 and 33 there is a limitation on the purposes for which information may be gathered. It may be gathered only for "police purposes" defined in s.21(3) of the Immigration and Asylum Act 1999 Act to mean the prevention, detection, investigation or prosecution of criminal offences, safeguarding national security and such other purposes as may be specified – see note to clause 32. No limitations are imposed on the purposes for which information may be disclosed to foreign law enforcement agencies under this section.

B. See the Immigration Act 2014

Biometrics

The Government Factsheet on biometrics[1] published with the Bill refers to implementation in summer 2014 and this is given effect by SI (2011/1820(C.81). There are powers (s 8) to require new categories of person to provide biometric data and new powers to carry out biometric checks.

The Factsheet says that the Government has no plans to place the Home Office's immigration biometric database under the oversight of the Biometrics Commissioner, arguing that biometrics held on this database are recorded for different reasons to those held on the police biometric database and that there are "existing oversight arrangements" although it is somewhat vague on these save for the comment "including the Information Commissioner".

The Government says in the Statement of Intent:

> 5. We intend to retain biometric information provided by foreign nationals for up to ten years from the date on which they enrolled their biometric information. However, different rules will apply where:
>
> i. the person becomes a British citizen; or
> ii. the person has indefinite leave; or
> iii. the person is subject to a Deportation Order, an Exclusion Order or a re-entry ban.
>
> b.…
>
> 7. The biometric information of foreign nationals who are granted indefinite leave will be retained while their leave continues. This is mainly to ensure that we can conduct anti-fraud checks should a person apply for immigration documentation or for citizenship. If their indefinite leave subsequently lapses or is revoked, the biometric information will be retained for up to ten years following the expiry of the leave or the date of the revocation.

8. We will retain biometric information from those foreign nationals who are subject to Deportation Orders, Exclusion Orders and re-entry bans for the duration of the order or re-entry ban where they exceed ten years.

Marriage and civil partnership

The marriage and civil partnership provisions are of the 2014 Act backed by extensive information sharing powers for the sharing of information between the Secretary of State and registration officials. A Policy Equality Statement (see the Equality Act s 149) is annexed to the Background Information paper.

The provisions permit the disclosure of information between registrars/registration authorities and the Secretary of State and from one registrar/registration authority to another. Registrars

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/249099/Factsheet_04_Biometrics.pdf

can disclose information for immigration purposes as (very broadly) defined and for purposes connected to the referral to the Secretary of State proposed marriage and civil partnership notices. The Secretary of State can disclose information and supply documents to registrars and registration officials for "verification purposes": the verification of information provided by a person giving notice of marriage or of a civil partnership and/or of the immigration status of a person who gets in touch with an official and/or whether the person is suspected of involvement in crime related to immigration and/or has been convicted of an offence relating to immigration. Information can be disclosed to a broader group of persons for "crime-fighting". Powers as to retention and disposal of information are similarly broad.

C. CIFAS

UKVI is a member of CIFAS. As such it can share data on individuals with private companies. The data may be held outside the jurisdiction and may be accessed by persons who are outside the jurisdiction. Some of the companies may be incorporated in countries other than the UK. The Home Office may both provide and receive data on individuals and those with whom it shares the data use, store and retain the data.

The companies who are members of CIFAS have many staff and these are spread across the globe. The chances of information about, for example, a person who has sought asylum or humanitarian protection falling into the hands of their persecutors appears to us high. Even if the person's initial claim for international protection was rejected, the sharing of the information may increase the risk to them taking them above the threshold whereby they are found to be in need of international protection. We recall what the Court of Appeal held in YB (Eritrea) v Secretary of State for the Home Department [2008] EWCA Civ 360 (15 April 2008) as to the lack of any requirement of affirmative evidence to establish certain aspects of the conduct of repressive regimes. In the case of those who remain in the UK but whose initial claims for asylum were rejected some time ago, circumstances in their country of origin may have deteriorated. The current difficulties with making further submissions, currently being litigated, mean that not all such people will have had an opportunity to make further submissions that are treated as a fresh claim for asylum. The dangers of providing not only an individual's personal biographical information but also an address in such cases are very clear.

There will be other migrants, in whose cases there is no risk of persecution, who could find themselves disadvantaged by the sharing of information between the Home Office and CIFAS. Fraud information and alerts posted by the financial services sector may not be accurate, or may not be sufficiently detailed to identify whether an individual has done anything wrong. That they should be used to make decisions on immigration applications, when the manner in which the data was gathered and its accuracy has not been verified to standards that would hold up in a court of law, creates a risk of unlawful conduct by the Home Office. The risk of discrimination on the grounds of race or nationality is high. We question whether the information held by the UK Border Agency is sufficiently accurate or complete to ensure that the financial services agencies with whom it shares information are not misled. In any event, no evidence is provided to demonstrate that a person's record with the UK Border Agency makes them a person of particular risk to a financial services agency.

Law on data protection

The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981) (ratified by UK in 1987) provides in Article 2 that "Personal Data' is defined as any information relating to an identified or identifiable individual - known in all subsequent texts as 'data subject".

Article 5 states that data is to be 'stored for specified and legitimate purposes' and not used in a way incompatible with these purposes (b); and is 'adequate, relevant and not excessive in relation to the purposes for which they are stored' (c) (emphasis added).

The length of time for which data is kept is to be 'no longer than is required for the purpose for which those data are stored.'
Article 6 describes 'special categories of data' including 'racial origin… health' which 'may not be processed automatically unless domestic law provides appropriate safe guards'.

Directive 95/46/EC (On the protection of individuals with regard to the processing of personal data and on the free movement of such data), requires Member States to enact domestic legislation on the processing of personal data to ensure and protect the fundamental rights and freedoms of natural persons as recognised under Article 8 of the European Convention and in the general principles of Community Law.

'Personal data' is defined in Article 2 (a) of the Directive by reference to whether information relates to an identified or identifiable individual, (as above). In addition to the Convention, the Directive details how 'reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity' are factors for identification.

Consent is stated in Section II, Article 7 to be necessary to make processing of data legitimate. It provides:

(a) the data subject has unambiguously given his consent OR
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into the contract… OR
(c) …compliance with a legal obligation to which the controller is subject OR
(d) …protect the vital interests of the data subject OR
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.

Article 10 describes information that is to be given to the data subject when collecting data from the data subject, including the purpose of the data collecting (10(b)), and the recipients or categories of recipients of the data (10 (c)). Article 11 details information that must be given to the data subject when not collected from him, including in 1(c) the recipients or categories of recipients.

The Data Protection Act 1998 repeats the substance of the Directive definition of 'personal data' in Part 1, 1(a) and (b). This is similar in wording to the Directive but with the added sentence that it 'includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'.[2]

The Act first considers the nature of the processing in order to determine whether the information in question is 'data' (either processed by automatic means or manual processing for a filing system) and, secondly, considers whether such 'data' is 'personal data' in that it relates to an identifiable individual. 'Sensitive Personal Data' means personal data relating to 'racial or ethnic origin of the data subject', as with the Directive.[3]

Schedule 3 states the conditions relevant to processing of the data. Processing data in order to protect the 'vital interest of the data subject or another person' is detailed in 3.3. Exceptions to consent are given in 3(a)(i) and (ii) whereby consent cannot reasonably be expected to be obtained (ii).

Schedule 3 also contains conditions for processing of data for legal proceedings (6(a)) and for the 'purposes of establishing, exercising or defending legal rights' (6(c)).

The length of time data is kept is stated as being assessed on a case by case basis in Part II, 7 (10). Here it is stated the 'prescribed period' means 40 days or such other period as may be prescribed and that (11) 'different amounts or periods may be prescribed under this section I relation to different cases'. The fifth principle of the Data Protection Act states that personal data should not be kept longer than is necessary for that purpose or purposes.

The relevant caselaw of the European Court of Human Rights includes the judgment of the Grand Chamber in S & Marper v UK (2008) (Application nos. 30562/04 and 30566/04) in which the Grand Chamber held:

> 'the core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage.' (para 107)

The Court stated that 'private life' covered physical and psychological integrity of a person (Pretty v UK, ECHR application 2346/022002) and that it can 'therefore embrace multiple aspects of the person's physical and social identity.'[4] The Court found that the 'mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8… and that the subsequent use of that stored information has no bearing on that finding (Amann v Switzerland ECHR application no. 27798/95 [2000]).[5]

The Court held that the individual's concern about the future use of stored data was legitimate and relevant to the determination of whether there had been an interference under Article 8.

[2] Part 1, 1, (1) (b). Data Protection Act, 1998.
[3] Part 1, 2, (a). *Ibid.*
[4] S66, *S.And Marper v The United Kingdom*, [2008] ECHR.
[5] S67, *Ibid.*

Different information is discussed as to what is considered sensitive or not; fingerprints are considered sensitive data and have the potential to impact on an individual's private life.[6]

The Court criticised the UK Government's 'vague' definitions regarding its procedures. It is essential to have clear rules governing the scope and application for measures, and 'minimum safeguards concerning duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction.'[7] An interference with Article 8 is considered necessary if there is a legitimate aim, and answers a 'pressing social need', and is proportionate to the legitimate aim pursued. Also the reasons adduced by the national authorities to justify it must be 'relevant and sufficient.'[8]

[6] S84. *Ibid*
[7] S99 *Ibid*
[8] S101.*Ibid.*