RESPONSE OF AMBERHAWK TRAINING LTD TO THE EUROPEAN COMMISSION'S CONSULTATION COMMUNICATION [*COM(2010)609*] CONCERNING THE DATA PROTECTION DIRECTIVE

FROM AMBERHAWK TRAINING LTD (Registered ID number: 50560025010-78)
DR. C. N. M. POUNDER,
JANUARY 2011
www.amberhawk.com
info@amberhawk.com

PART 1: Introduction and summary

Introduction: who or what is "Amberhawk"?

Amberhawk Training Ltd is a company founded in 2008 by Dr Chris Pounder and Sue Cullen as the vehicle for the continuation of the information law training business previously operated by Pinsent Masons LLP. Its main business is designing and delivering information law training – in data protection, freedom of information, information security, human rights, the Regulation of Investigatory Powers Act, marketing rules and related areas of law. Amberhawk also provides a topical privacy blog (Hawktalk).

The author of this document has been involved in data protection for three decades. For ten years prior to joining Pinsent Masons, he headed an Information Privacy Consultants team whilst working for Cap Gemini, a leading IT supplier in Europe. There, he developed courses in a number of security and data protection issues and produced and edited the specialist quarterly magazine *Data Protection News*. Prior to that, Chris was in charge of the Data Protection Team at the Greater London Council and London Residuary Body.

Dr Pounder's interest in data protection dates back to 1978. He has spoken at numerous conferences on data protection and related matters and also writes the occasional freelance article for the IT-related Press and the academic journals in the field of security and data protection. He has also given oral and written evidence before various Parliamentary Select Committees where issues of privacy, data protection and security have arisen (e.g. ID Cards, Computer Misuse Act, data retention policies, supervision of the national security agencies).

Amberhawk's response does not cover all the questions found in the consultation document We have no objection to this document being made public or being published by the Commission. If the Commission want to explore some of the ideas being expressed here, Amberhawk would be delighted to assist.

Summary of our main conclusions

1. **Personal data**: There should be an extension of the definition to include employment records so that **any** manual information on employees gain full protection from the Directive.

2. **Personal data**: the definition should include the situation where the data subject can provide the identification details that the data controller lacks. This change is relevant to the question of whether or not an IP addresses, URLs etc etc should be treated as personal data and places the data subject in control over his own privacy when using the internet.

3. **Sensitive personal data/biometrics**: two UK Courts have concluded that photographs of data subject are likely to be sensitive personal data as they display racial features (e.g. skin colour). The proposed change ensures that ordinary personal data can become sensitive personal data if there is a processing objective to reveal details of an individual's health, race etc. The change would also be useful in the determination of whether or not an individual's biometric is sensitive personal data of not.

4. **Notification/Accountability Principle:** The bureaucracy can be simplified, used far more constructively to promote Codes of Practice, provide more meaningful description of purposes and disclosures to Recipients, and can also be used to regulate an Accountability Principle.

5. **Human Rights link**: the Data Protection regime should be explicitly linked regime with Article 8 of the Human Rights regime. In this way, a Data Protection Authority should be able to use his powers in cases such as the retention of personal data on a national DNA database.

6. **Law Enforcement and National Security exemptions.** The Data Protection Authority has to have effective powers of intervention and be able to raise cases of substantial public interest concerning the application of any law enforcement/national security exemption.

PART 2: Detailed analysis

The following text links the above conclusions to the Consultation Document in three areas:

1. Ensuring appropriate protection
2. Sensitive data
3. Administrative burden

ENSURING APPROPRIATE PROTECTION (2.1.1)

1. Inclusion of manual employment records as personal data

Manual records containing personal information associated with an individual's employment should always be subject to a data protection regime – this is not the case as the Directive permits Member States (e.g. the UK) to exclude manual employment records from a data protection regime. ***At the very least***, and a time of great uncertainty with respect to employment, all manually employee records held by employers should be subject to the right of access and correction.

To leave manual employee records unprotected leaves a glaring privacy loophole which allows both public and private sector employers evade all data protection obligations; it is a loophole that any future "Consulting Association"[1] could exploit..

The Commission should close the manual files loophole in general, but especially in connection with manual employment records.

2. Redefinition of personal data

It is convenient to start with the kind of definition of personal data that could emerge (the example is an addition to the current UK definition in ***italics***):

[1] See http://www.computerweekly.com/Articles/2009/06/03/236244/ICO-closes-down-illegal-blacklist-database.htm (one story of many which covers this Association).

> "**personal** data" means data which relate to a living individual who can be identified-
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, ***or***
>
> (c) ***from the data and other information which has been provided by, or is likely to be provided by, the data subject***.

The change allows personal data to be redefined to include the situation where the data subject can provide the identification details that the data controller lacks. This change is especially relevant to the question of whether or not an IP addresses, URLs etc etc should be treated as personal data.

The effect of this change is to empower data subjects. For instance, if an image in Google Street View appears and the data subject informs Google and says "this is me on Street View, this is my identity and this is the relevant URL", then the image becomes "personal data" and subject to data protection law. Similarly with IP addresses: if the data subject says to an ISP that "at such and such a time, this IP address was used by me" and "I prefer not to be tracked or to be sent marketing messages".

Note that the fact that the IP/URL data become personal data does **NOT** mean that the personal data have to be deleted or that the processing **has** to cease. Data protection creates a balance between the individual concerned and the organisation in control of the processing. As with all balancing acts, the facts associated with the processing of personal data will determine in which direction the scales will tip.

The objective of the change in the definition is to ensure the national data protection law is engaged, so that any balancing of interests can occur. The objective is **not** to determine where the balance falls. Note also the change empowers the data subject who decides when, or if, to make IP-type data, personal data. If everyone was happy with an ISP's privacy arrangements then there would

be no need for data subjects to notify the ISP[2] of their identity. By contrast, if there were to be any privacy controversy, then many data subjects would be able to protect themselves by providing the necessary identifying details (e.g. at the start of an internet session).

The technical details needed to be provided by a data subject will not be onerous, and it is to be expected that the "privacy lobby" will develop a range of free Apps that allow data subjects to provide the necessary identities and technical detail associated with their browsing habits.

3. Link to Article 8 of the Human Rights Convention

Issues surrounding "lawful processing" in terms of Article 8 of the European Convention of Human Rights do not form part of the Consultation yet this matter is very important because such processing is identified as part of the text of the Directive. For example, Article 1, defines the purpose of the Directive in these words: "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their *right to privacy* with respect to the processing of personal data".

Recital 1 adds further clarification in that the Directive is a step towards "...preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms".

Recital 10 then amplifies what is meant by the "*right to privacy*". It states that "... the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the *right to privacy*, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights

[2] For further detailed argument see the document "**Reclaiming Privacy on the Internet"** which describes how individuals can protect their internet browsing by engaging a data protection regime; IP addresses and URLs linked to user sessions can be transformed into personal data at any time by the user) http://www.amberhawk.com/policydoc.asp

and Fundamental Freedoms". Recital 11 then adds that "*the right to privacy*" in the Directive is intended to "give substance to and amplify those (provisions) contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data".

In other words, the Data Protection Authority should be able to enforce its national law in circumstances when Article 8 is concerned with the processing of personal data. It should be possible for the Data Protection Authority to assess whether or not some processing is lawful (e.g. proportionate) in terms of Article 8. For example, the Data Protection Authority in the UK should have been involved, on data protection grounds, in the case of *S & Marper v UK* and the DNA database or the retention of personal data on that database.

In the UK, the Article 8 right that relates to the processing of personal data could be implemented as an amendment to the Sixth Data Protection Principle. For example:

> *"Personal data shall be processed in accordance with the rights of data subjects under this Act and, in particular, personal data shall not be processed in a way that does not respect the private and family life or correspondence of data subjects".*

Obviously this Principle has to be qualified in a way that engages the exemptions found in Article 8(2) of the Human Rights Convention (i.e. provide appropriate exemptions for national security, law enforcement etc).

By implementing a right to the privacy of personal data under the auspices of a right, the processing of personal data for freedom of expression purposes should be left undisturbed[3]; investigative journalism, for example, is unaffected by the change.

[3] Section 32 of the DPA provides a wide exemption for freedom of expression (e.g. all rights, Principles except the security obligations) but only until the point of publication of the personal data concerned.

The effect of this change would explicitly link the Human Rights and Data Protection regimes and give the UK's Information Data Protection Authority an explicit human rights role but only in the context of the processing of personal data.

4. Proper supervision of law enforcement agencies.

Any revised Directive must ensure that a regulator with privacy responsibilities in the area of national security and law enforcement is equipped to make effective interventions (e.g. the regulator must be able to investigate issues of public interest concerning the application of the data protection rules to surveillance or to law enforcement/national security operations, and be able to examine the relevant personal data or interview staff).

Any new Directive ***should not*** allow Member States the flexibility to draft exemptions so wide that it allows them to negate any privacy protection the Commission seeks to introduce. Identification of the powers of the regulator in these areas would help harmonise third pillar activities as part of the drafting of the Directive, and minimise the need to have the Commission involved in the post-implementation harmonisation procedures that are identified in its discussion document.

5. Recovery of costs

A Data Protection Authority should be able to recover, if appropriate, the costs associated with any enforcement activity (e.g. in the UK these are Information Notice, Monetary Penalty Notice or Enforcement Notice). At a time of austerity, this is important. If we expect a Data Protection Authority to protect the privacy of individuals, that Authority should not be financially penalised when it does.

The possibility of costs recovery will also encourage data controllers to co-operate with the Data Protection Authority to avoid him invoking costs by issuing a formal Notice. Finally, the legal process should also be able to award costs to the Data Protection Authority if warranted.

SENSITIVE DATA (2.1.6)

1. Special Personal Data definition

The definition of "special category" of personal data outlined in Article 8 of the Directive ("sensitive data" or "sensitive personal data") should be not be changed. Instead there is a suggested change that permits ordinary personal data to become sensitive personal data if they are processed in a way that reveals something about a data subject's health, trade union membership etc.

This is done by adding something like the following provision to Article 8:

> *"**personal data**" become "**special personal data**" if they are processed by a data controller, or intended to be processed by a data controller, for a purpose that reveals, or is intended to reveal, a data subject's health, trade union membership, criminal conviction, racial origin etc*

In the UK there are emerging problems with the definition of "sensitive personal data" (the UK name for "special category" personal data). In *Naomi Campbell*[4], the Court toyed with the idea whether or not a photograph was sensitive personal data because the data subject was black. In *Murray*[5] the Court concluded that photographs of identifiable individuals were sensitive personal data but in this time the data subject was white.

The kind of change proposed would require that the items of sensitive personal data currently listed in Article of the Directive, to be qualified by a processing objective that was to "reveal" a data subject's health, race, criminality etc. In other words, the context in which the processing occurs is an important factor as well as the content of the personal data. The current definition focuses only on the latter.

It could be that the word "reveal" might not be the most appropriate word, but an example should clarify what is intended. Suppose a data controller has a set of names and addresses – these are not special personal data as the personal data do not consist of the items of personal data described in A.8 of the Directive. However,

[4] Para 85 of [2002] EWHC 499(QB): Campbell v Mirror Group Newspapers

[5] Para 80 of [2007] EWHC 1908 – Murray v Express Newspapers and Big Picture

if the data controller were to process name and address information to identify all the Cohens, Steinbergs, Aronowitz's etc, it would be processing personal data in a way intended to identify Jewish people and their address (e.g. in order to tell them of the data controller's Jewish Delicatessen that has just opened). This would become the processing of sensitive personal data.

So it is not enough to take a photograph of an individual to have "sensitive personal data re race" (as per the two UK judgements referred previously). The data controller has to process the personal data within a context that needs the race (e.g. the data controller actually wants to process photographs to distinguish the black Fred Bloggs rather than the white Fred Bloggs, or which Fred Bloggs has smallpox spots on the face).

2. Inclusion of biometrics

This approach also resolves the issue of the use of biometrics and whether biometrics should be classified as items of special personal data. If biometrics personal data are used to "reveal" say a racial profile or a health condition (e.g. DNA shows a predisposition for breast cancer), then the personal data are special personal data. If the biometric is used as an identifier for some security process, then it is not.

The issue of whether or not a biometric should be processed can also be determined by the Adequacy/Relevant/Excessive Principle. For example, it would be excessive to process personal data that represents fingerprints to the degree needed by the police (i.e. to identify one individual in several million) when the data controller only wanted to administer free school dinners where the requirement was to identify one individual in a five hundred.

ADMINISTRATIVE BURDEN

1. Notification and an Accountability Principle.

Notification could be used to help implement any Accountability Principle, if the data controller has to answer as part of notification renewal, an brief compliance check-list (e.g. below) relevant to the Accountability Principle.

ILLUSTRATIVE ACCOUNTABILITY QUESTIONS THAT COULD APPEAR

Has the data controller adopted appropriate policies and management structures that ensure that data protection and security have a prominent role?
Has the data controller taken all appropriate steps to control physical security?
Has the data controller taken all appropriate put in place controls on access to personal data?
Has the data controller established a business continuity plan? (for example, holding a backup file in the event of personal data being lost through flood, fire or other catastrophe)?
Has the data controller trained all its staff on all relevant operating procedures involving personal data including security procedures, and that this obligation applies to data processors contracted to it?
Will the data controller report to the Data Protection Authority any significant loss of personal data or other significant breaches of the Principles by any cause (e.g. accidents, theft, lost laptops)?
Does the data controller have a policy of detecting or investigating breaches of security and other processing procedures when they occur?
Has the data controller appointed a member of staff or agent who has a data protection role as part of his job description or responsibilities?
Does the data controller review data protection policies, standards and procedures on a regular basis?
Has the data controller integrated data protection procedures and data subject rights into the procurement process?
Have security and privacy risk assessments been undertaken?
Has the data controller adopted ISO27001, HMG Security Framework or equivalent?

The Questions above are not meant to be complete list – they comprise an illustrative list to show how it could assist compliance with any accountability/security requirement if the statement has to be resubmitted as part of the registration renewal cycle. The answer to these Questions should form part of the public part of the register.

2. Making Notification (Registration) more relevant

Notification can be used far more constructively than it is and can be used constructively to promote Codes of Practice. Notification can be clarified so the content of the public register is more meaningful. Finally, the public register has to

remain as it is a mechanism for data controllers to acknowledge the fact they have data protection responsibilities.

(a) **Codes of Practice**: A data controller should be able to notify part of its processing by reference to an appropriate Code of Practice (if it exists). The Codes in mind are those approved either by the Secretary of State. European Commission or the Data Protection Authority. This step would also enhance the status of Codes of Practice and simplify registration. For example, registration of a data controller with respect to CCTV, employment, and other Codes in future could be reduced to a few lines (e.g. a data controller contact details, Codes of Practice A, B, C and D). Registering by reference to a Code of Practice is evidence that the data controller knows about the Code and by implication its details. This could be useful of there is an issue associated with adherence to the Code or enforcement of the Principles.

(b) **Purposes and disclosures to Recipient(s):** Where purposes have to be registered by a data controller, one could have a marker in the notification which indicates that the processing purpose occurs for a reasons **other than** (a) consent of data subject or (b) necessary for a statutory function, or obligation of a public authority or Government Department, or the administration of justice[6]. The same could apply to a registered disclosures of personal data to a Recipient.

This provides a mechanism to identify to the public in the register, those purposes and Recipients that fall outside the normal processing parameters. It shortens notification and also identifies them to data controllers, who should be alert to the implication that the marked purpose or Recipient might need to be justified.

Dr C. N. M. Pounder
Amberhawk Training Ltd
January 2011

[6] The conditions associated with Schedule 2 of the UK Act, paras 1, 3, 5(a)-5(d) but not 2, 4, 5(e) and 6.