

RESPONSE OF AMBERHAWK TRAINING TO THE MoJ CONSULTATION ON THE CURRENT DATA PROTECTION LEGISLATIVE FRAMEWORK



A DATA PROTECTION ANALYSIS
FROM AMBERHAWK TRAINING LTD
DR. C. N. M. POUNDER, NOVEMBER 2010



AMBERHAWK

www.amberhawk.com

PART 1: Introduction and summary

Introduction

Amberhawk's response does not cover all the questions found in the consultation document and, at the end, we make a few comments that relate to issues not raised by the consultation. We have no objection to this document being made public. Some of the suggestions (e.g. recovery of costs by the Commissioner) do not need to wait six or so years for the new Directive to be agreed and implemented.

We have also addressed the issues using the context of the Data Protection Act 1998 so they become less theoretical or distant.

Summary of our main conclusions

- 1. Personal data:** There should be an extension of the Accessible Records definition to include employment records so that manual information on employees gain full protection from the Act. This would close an obvious loophole at a time when public and private sector organisations are facing difficult economic times and are likely to shed staff.
- 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. Personal data:** the definition should be changed to remove all the confusion caused by *Durant*. This can be done by removing the reference to the text that relates to "opinions" and "intentions".
- 4. Sensitive personal data/biometrics:** two 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 to be sensitive personal data, there has to be a processing objective to reveal something about an individual's health, race etc. The change is also useful in the determination of whether or not an individual's biometric is sensitive personal data of not.

- 5. 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.
- 6. Data Protection Principles (First, Sixth):** the Sixth Principle should be used to explicitly link the Data Protection Act with Article 8 of the Human Rights Act. In this way, the Information Commissioner should be able to use his powers in cases such as the retention of personal data on a national DNA database.
- 7. Powers of the Commissioner.** There needs to be a mechanism where the Commissioner can serve an administrative notice (a "Data Protection Practice Notice") requiring a data controller to take certain steps by a certain time to ensure that any processing of personal data is in accordance with the Act. The data controller has the right of appeal to the Tribunal against the Notice **and** the data subject has a limited right of appeal to the Tribunal against the ICO's decision not to serve a Notice. This mechanism is modelled on the FOI Decision Notice regime.
- 8. Powers of the Commissioner:** The Information Commissioner should have the discretion, subject to appeal to the Tribunal, to be able to recover the costs associated with any Audit or Notice he issues. If we expect the Commissioner to protect individuals, then he should not be financially penalised when he does. In a time of austerity, this is especially important.



- 9. The Special Purpose(Section 32 of the Act).** The Government should take the opportunity to ensure that the S.32 exemption applies only to that processing of personal data that occurs before publication. This was the intention of Parliament when Section 32 was first introduced into the Data Protection Bill.
- 10. The National Security exemption (Section 28 of the Act).** The exemption should be changed to allow a Tribunal to hear the Commissioner's case if he raises a matter of substantial public interest concerning the application of the national security exemption.
- 11. Merging of Regulators:** The Government should explore whether there are savings to be made, and privacy benefits to be gained, in merging the office of the Information Commissioner, Interception of Communications Commissioner, Surveillance Commissioner and the privacy interests of the Human Rights Commission and Financial Services Authority.
- 12. Comments on the Consultation and Directive 95/46/EC:** The detail about the infraction proceedings against the UK and areas of disagreement in relation to the implementation of Directive 95/46/EC should have been explained prior to the consultation. This is especially the case if the Consultation questions related to issues subject to possible proceedings.



PART 2: Detailed analysis

The following text links the above conclusions to the specific questions of the Consultation Document.

Q2: Comments on the definition of personal data

A. Extension of Accessible Records to employment records (Q2)

Manual records containing personal information associated with an individual's employment should become an Accessible Record and fully subject to the Act. At the very least, manual employment records should be defined to be a special form of category(e) data which can be processed by **any** data controller.

At a time of great uncertainty with respect to employment, all manually held employee records, should be subject to the right of access and correction. A consequence of this suggestion is that Section 33A(2) of the Data Protection Act (introduced by the Freedom of Information Act 2000) should be repealed.

To leave manual employee records within their current status under the Act leaves a glaring loophole which allows both public and private sector employers to process personal information in a reasonably structured manual file and evade all obligations in the Act; it is a loophole that any future "Consulting Association"¹ could exploit.

Making employee records fall within the ambit of an Accessible Record is far more effective than the last Government's promotion of a narrowly drawn, prohibited list established by the Employment Relations Act 1999 (Blacklists) Regulations 2010.

B Redefinition of personal data (Q2)

It is convenient to start with the kind of definition of personal data that should emerge (additions to the current definition in **italics**, deletions with ~~strike out~~):

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.

~~and 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;~~

There are two changes to suggest.

- The first change is that personal data should be redefined to 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.
- The second change is to recognise that the Court of Appeal in *Durant*² narrowed the definition of "personal data" by reference to the text in the definition of personal data that related to "opinions" and "intentions". This paragraph ("and includes any expression ...") should be removed.

The effect of the first 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 the Act. 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".

Note that the fact that the data are 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.

² *Durant v the FSA*, Case Reference [2003] EWCA Civ 1746



The objective of the change in the definition is to ensure the Act 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 ISP³ 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.

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.

The effect of the second change is to remove any *Durant* legacy. In *Durant*, the Court of Appeal somehow overlooked the intention of Parliament as clearly expressed in the House of Lords by Ministers when it enacted this provision by amendment. Instead, the Court used the "opinion and intention" text to justify an interpretation that, in practice, has narrowed the scope of personal data and manual files subject to the Act. It is worth noting that it was *Durant* that was the main trigger for the European Commission's infraction proceedings against the UK.

Q7: Sensitive Personal Data and inclusion of biometrics.

The definition of "sensitive personal data" should be changed so that the current phrasing is less ambiguous. At the moment the definition begins; "In this Act **"sensitive personal data"** means personal data consisting of information as to....."

The suggested change makes the definition of sensitive personal data something like:

³ For further arguments 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>



"In this Act "sensitive personal data" means personal data **that are processed, or intended to be processed, for a purpose that reveals an individual's....."**

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 Section 2 of the Act, to be accompanied with 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 sensitive personal data as the personal data do not consist of the items of personal data described in S.2 of the Act. However, 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 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).

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*



This approach also resolves the issue of the use of biometrics and whether biometrics should be classified as items of sensitive personal data. If biometrics personal data are used to “reveal” say a racial profile, then the personal data are sensitive 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 be determined by the Third 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.

Q26: Notification (Registration) to the ICO

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 or the Information Commissioner (ICO) (the latter obviously includes the ICO’s own Codes of Practice). 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 if there is an issue associated with adherence to the Code or enforcement of the Principles.



(b) **Purposes and disclosures to Recipient(s):** Purposes registered by a data controller 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 justice⁶. 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 also identifies them to data controllers, who should be alert to the implication that the marked purpose or Recipient might need to be justified.

Q26:Notification/Registration & an Accountability Principle.

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

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 Commissioner 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 are not meant to be complete list – just an illustrative list.

⁶ The conditions associated with Schedule 2, paras 1, 3, 5(a)-5(d) but not 2, 4, 5(e) and 6.



It will assist compliance with any accountability/security requirement if the statement has to be resubmitted as part of the yearly, registration renewal cycle.

Q26 : Notification (Registration) – a legal problem.

The Courts have equated the “purpose” of the processing as used in the Data Protection Principles (e.g. the Second, Third, Fifth Principles) with the “purpose” as notified⁷ to the Commissioner. However, as the purposes defined in notification/registration procedures are very broad and serve a different function, then this equation effectively undermines the protection afforded to data subjects by the Principles that rely on the word “purpose” for their effect.

For example, suppose we are looking at the Third Principle and whether or not an item of personal data is relevant to, say, the “housing benefit” purpose. If the purpose that relates to the Third Principle is equated to the purpose defined for “registration/notification” in the ICO Notification Handbook then the purpose expands away from “housing benefits” to “Benefits, grants and loans administration” in general. In this way, an item of personal data that could be viewed as excessive in the context of “housing benefits” can be argued as being relevant to “benefits administration” in general⁸.

It should be noted that the Court’s decision is not in accord with Directive 96/46/EC; this Directive does not link the provisions that relate to notification with the provisions that define the Data Protection Principles.

Q31 Powers of the Commissioner (lawful processing)

Issues surrounding “lawful processing” do not form part of the Consultation yet this matter is very important because “lawful” processing forms part of the text of three Data Protection Principles (1st, 2nd, 7th). Any backing-off the enforcement

⁷ *Humberside Police etc v ICO* (Court of Appeal) [2009] EWCA Civ 1079

⁸ For further details as to how the Principles could be undermined see <http://amberhawk.typepad.com/amberhawk/2009/11/could-notification-to-the-commissioner-undermine-three-data-protection-principles.html>



of “lawful processing” would therefore degrade the protection afforded to all data subjects⁹. Sadly the Information Commissioner for very understandable reasons does not appear to enforce lawfulness.

This abstinence is contrary to Directive 95/46/EC which, in 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 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 Commissioner should be able to enforce the Act in circumstances when Article 8 is concerned with the processing of personal data. It should be possible for the Commissioner to assess whether or not some processing is lawful in terms of Article 8. For example, the Commissioner should have been involved, on data protection grounds, in the case of *S & Marper v UK* and the DNA database and the retention of personal data on that database.

⁹ See <http://amberhawk.typepad.com/amberhawk/2010/04/information-commissioner-should-enforce-article-8-privacy-rights.html>



In the UK, the Article 8 right that relates to the processing of personal data should 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). There is also a need to modify the Human Rights Act so that any issue with respect of personal data is treated under the Data Protection Act.

By implementing a right to the privacy of personal data under the auspices of the Data Protection Act, the processing of personal data for the Special Purpose (i.e. freedom of expression purposes) will be left undisturbed¹⁰; investigative journalism, for example, is unaffected by the change.

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

Q31 Powers of the Commissioner – Practice Notice

There has been, since 1984, about 15 Tribunal hearings into data protection matters. By contrast, since 2005, under the Freedom of Information (FOI)/Environmental Information Regulations (EIR), there have been 33 Tribunal hearings (5 per year) relating to the data protection/freedom of information

¹⁰ Section 32 of the DPA was introduced by Parliament with the intent of protecting the Press but only until the point of publication of the personal data concerned. However the Court has determined that the exemption is not limited in this way – see reference 11.



interface. The result is that the legal framework that surrounds the workings of the Data Protection Act, is often interpreting the law within an FOI/EIR context.

The Information Commissioner, in terms of FOI, releases scores of Decision Notices per year but very little (except for the voluntary Undertakings) on data protection.

The result is that data controllers cannot properly understand how the Act works in practice and learn what the Information Commissioner has determined in the context of data protection investigations. The Courts, for its part, cannot be informed, in its judgments, by the Tribunal's careful consideration of often very technical data protection matters. This probably explains why, in the context of Data Protection, the Courts often make determinations which many find "curious".

The Commissioner has partially addressed this problem by publishing formal Undertakings, signed by data controllers following a data loss. But this is a voluntary arrangement and provides little legal analysis and focuses on the 7th Principle. In addition, a kind of "unfairness" is beginning to arise. For example, in the Tunbridge Wells Equitable Friendly Society Limited Undertaking¹¹, the data loss arose by the sending of very confidential details to the wrong individual. However, one can see equally catastrophic results relating to untrained staff having access to a single record, or staff updating a single record incorrectly, or staff not deleting the required record but these equally damning consequences would not attract an Undertaking because there had been no data loss.

A consistent approach can be achieved by introducing a "Data Protection Practice Notice" mechanism in data protection regulatory regime. This is an administrative notice served by the Commissioner requiring a data controller to take certain steps by a certain time to ensure that any processing of personal data is in accordance with **any** Data Protection Principle. The data controller has the right of appeal to the Tribunal against **and** the data subject has a limited right of appeal to the Tribunal against the ICO's decision not to serve a Notice.



In effect this formalises the Undertaking arrangement but **adds** a route of action for the data subject. So where there is an issue of **substantial** public interest (e.g. recently contested issues surrounding Google Street View), data subjects or persons representing data subjects should be able to challenge the content of a Data Protection Practice Notice, or the refusal of the Commissioner to serve such a Notice.

Q31 Powers of the Commissioner (recovery of costs)

The Information Commissioner should be able, at his discretion, to recover the costs associated with any Audit undertaken by his office, or any Notice that he issues (e.g. Information Notice, Monetary Penalty Notice or Enforcement Notice). At a time of austerity, this is important. If we expect the Commissioner to protect the privacy of individuals, he should not be financially penalised when he does.

The possibility of costs recover will also encourage data controllers to co-operate with the Commissioner to avoid him invoking costs by issuing a formal Notice. Finally, the Tribunal should also be able to award costs to the Information Commissioner if the appeal before the Tribunal warrants it.

Q100 – Four other issues:

The Special Purpose – Section 32 of the Act. The Government consider whether to take the opportunity to ensure that the Section works in the way Parliament intended it to work (i.e. follow the agreement between Lord Wakenham for the Press Complaints Commission with the Government of the day as endorsed by Parliament when the Bill was before Parliament). Lord Phillips¹² (para 127 and 128 of Naomi Campbell) has made an interpretation of section 32 which effectively ignores this agreement which said the exemption only applied **prior** to publication, to one that continues **after** the time of publication.

¹¹

http://www.ico.gov.uk/upload/documents/library/data_protection/notices/the_childrens_mutual_undertaking.pdf

¹² Para 128 of [2002] EWCA 1373: Campbell v Mirror Group Newspapers



The National Security exemption – Section 28 of the Act. A recent judgment from the National Security Tribunal (with Privacy International)¹³ concluded that the Tribunal only had jurisdiction if the complainant was “a person directly affected” by the processing and this meant somebody like a data subject undertaking a subject access request and who was refused access. Privacy International was raising an issue not concerned with about subject access but about the general application of the 2nd and 8th Data Protection Principles applying to thousands and thousands of data subjects. The result was that Privacy International could not progress their appeal.

The S.28 exemption should be changed to allow a Tribunal to hear the Information Commissioner whenever he raises a matter of **substantial** public interest concerning the application of the national security exemption.

Merging of Regulators: The Government should explore whether there are savings to be made and privacy benefits of merging the office of the Information Commissioner, Interception of Communications Commissioner, Surveillance Commissioner and the privacy interests of the Human Rights Commission and Financial Services Authority. There are good reasons for this step¹⁴.

Comments on the Consultation and Directive 95/46/EC: The detail about the infraction proceedings against the UK and areas of disagreement in relation to the implementation of Directive 95/46/EC should have been explained prior to the Consultation. This is especially the case if the Consultation questions related to issues subject to possible proceedings.

Dr C. N. M. Pounder
Amberhawk Training Ltd
November 2010

¹³ <http://www.informationtribunal.gov.uk/Documents/nsap/PrivacyInternationalweb.pdf> - For issues with respect to the Second and Eighth Principles, see details on <http://amberhawk.typepad.com/amberhawk/2009/10/can-national-security-agencies-disclose-communications-data-or-anpr-images-to-anybody.html>

¹⁴ See <http://amberhawk.typepad.com/amberhawk/2010/10/spending-review-why-not-axe-the-information-commissioner.html>