RECLAIMING PRIVACY ON THE INTERNET

(IP ADDRESSES, REFERENCE NUMBERS, URLs AND THE UK's DATA PROTECTION ACT 1998)

AMBERHAWK

A DATA PROTECTION ANALYSIS
FROM AMBERHAWK TRAINING LTD
DR. C. N. M. POUNDER, JULY 2009

RECLAIMING PRIVACY ON THE INTERNET

PART 1: MANAGEMENT SUMMARY

OVERVIEW

There is a current, lively debate as to whether data that contains no name but is linked to an Internet user session via an IP address, URL or similar reference number is personal data or not. If the data **are not** personal data, then the person who controls the data has almost untrammelled power to decide the nature of the processing. By contrast, if the data **are** personal data, that controller would be constrained by the data protection obligations that serve to protect the privacy of the individual users concerned.

For example, whereas an organisation can freely process data not linked to an identifiable individual to achieve any marketing or promotional objective, this is not the case if the data are personal data and the right to object to the marketing purpose is engaged.

This analysis helps answer the central question is: "Can such data be linked to an identifiable user, especially in the absence of a name?". It shows that individual users can ensure that such data can become personal data **unambiguously**.

A full legal analysis is presented in the context of the UK's Data Protection Act and includes advice for service providers, for data subjects, and discusses possible counter arguments. This analysis is valid for countries where the national data protection legislation is based on the Data Protection Directive 95/45/EC or on the OECD Guidelines; Google's privacy policy suggests that the analysis applies to it. The analysis takes account of likely counter arguments.

SUMMARY OF THE MAIN DATA PROTECTION EFFECTS

In outline, an individual user can, at any time, send an Internet service provider his name, address, time the service was used, and any relevant URL, reference number or IP address associated with that user session. If this information is sent, then the service provider possesses all the identifying information needed to link any related service data or profiling data derived from a user session to that individual. That individual has become **unambiguously** identifiable and any **further** processing of the personal data related to the user session will engage the usual data protection obligations.

As more and more users of a service send a service provider these details, there will become a threshold of user contact after which a service provider should assume that personal data are processed on **ALL** users of a service without the need for user identifying information to be sent. This is because the rate of user contact is such that a service provider can anticipate that he is likely to be sent the identifying information about an individual user.

There is now a simple test of whether or not certain information linked to an IP address, reference number or URL is personal data. If the individual user concerned provides the necessary identifying information, then the data ARE personal data. If sufficient individual users each provide the necessary identifying details, then the data linked to ANY individual should be considered to be personal data.

The article stresses that because a data protection regime is engaged, it does not mean that a service provider has to delete the personal data or halt its processing, or that the individual concerned somehow gains the upper hand. All it means is that the service provider has to be mindful of the data protection obligations when deciding to process the personal data concerned.

If there is doubt as to whether these obligations are being implemented properly, then the Information Commissioner could be asked for an assessment as to whether this is the case. As with all assessment processes, it cannot be concluded that the outcome will always automatically favour the individual user concerned. However, it has to be recognised that the fact that a data protection regime can be applied represents a shift in power. As soon as the data become personal data, the individual concerned is empowered to apply those parts of the Act that can protect his interests in any **further** processing.

> ***Individual users can, at any time, seek the protection of a data protection regime by providing the necessary identifying details to any organisation that stores their IP address or URL. Organisations will have to adjust their procedures to take account of the reality that any subsequent processing is the processing of personal data.***

The detailed conclusions that impact on service providers

a) Service providers are processing personal data if they have data in their possession that relates the use of a service to an identified living user of that service. In such circumstances data protection legislation would apply. This position is self evident from the definition of personal data and is only mentioned here for completeness.

b) Service providers will also be processing personal data if they can anticipate that the information that identifies a living individual is **likely**[1] to come into their possession (e.g. if staff are likely to look up details about an individual user from any source, or to obtain identifying information from a third party). This position is also self evident from the definition of personal data and is only mentioned here for completeness.

[1] *"Likely" is somewhere in between "possible" and "probable" (e.g. reasonably foreseeable; something which has a good chance of occurring)*

c) In the absence of "other information" that identifies an individual, or the likelihood of obtaining such information, or the receipt of the identifying detail from an individual, service providers are **unlikely** to be processing personal data.

d) Assuming that the processing does not fall within (a) or (b) above, there is a simple mechanism that can be used by any individual user to transform information such as an IP address or URL into personal data. All the individual needs to do is provide the relevant identifying information to the service provider (e.g. name, IP address, date, time of use of service etc), preferably accompanied with a complaint of substance about the processing.

e) The ability of an individual to contact the service provider in order to identify that certain data relates to him is a natural consequence of Recital 26 of the Directive. Once an individual is identified in this way, any **further** processing of the data is the processing of personal data.

f) If more and more individuals contact a service provider in order to disclose identifying details described in (d) above, the more a service provider should anticipate that identifying details will come into his possession, and the more and more the situation will resemble that described in paragraph (b) above. This prospect arises because the frequency of contact from individuals has changed from "contact that is possible" to "contact that is likely". When this change occurs, the number of contacts or the frequency of contact is such that a service provider should treat ALL the data as personal data (i.e. without the need for any further contacts).

g) Service providers who process IP addresses in connection with marketing related activities should, if the mechanism in (d) is used, satisfy the right to object to marketing purpose. If contact is "likely" as described in (f), service providers should anticipate that prior consent for the marketing purpose is generally required. These conclusions are a consequence of the individual's strong right to object to the processing of personal data for a marketing purpose, as granted by data protection law. The arguments with respect to a marketing purpose are not dependent on the consent requirements of the Privacy in Electronic Communications Directive[2].

h) Service providers should expect that the procedure described in d) could apply a data protection regime to cookies and transient IP addresses etc.

i) Service providers should expect the development of software applications to ensure that data used in connection with the use of a service can be linked

[2] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.*

to identifying information about a user which are then automatically sent to the service provider, prior to the commencement of a user session. Such applications would automatically transform data into personal data.

j) Service providers should expect that some individuals may be able to exercise the right to object to the processing of their personal data. However, as the right to object to the processing of personal data is limited and it does not apply universally (e.g. if personal data about internet communications are necessarily retained for law enforcement purposes).

k) Service providers should expect that retention policies with respect to IP address, web-searches can become regulated by a data protection regime. Personal data are no longer data that can be retained by a service provider for an arbitrary period (for example, a period beyond that which is required by law or in connection with national security or by law enforcement agencies).

PART II: THE DETAILED ANALYSIS

INTRODUCTION

Without doubt services such as Google Street View can be useful. Just imagine that you are going for a job-interview in an unfamiliar city-centre; isn't it useful to know the lay of the land before you travel? However, away from the city centres, some householders claim that Google's Street View has invaded their private space by publishing pictures that can zoom through the upstairs windows or into front rooms. Sometimes, privacy campaigners have based their data protection arguments on the processing of images that show shadowy Street View figures in a compromising poses. On the other side of the argument, there are many who can't see what the privacy problem is. "What is the difference", they argue, "between Street View image or an image on the TV screen or the holiday photographs taken by tourists that include crowded shopping centres or on the beaches?".

This analysis does not want to enter this debate; all it concludes is that if the data are personal data, any argument can be resolved by a data protection regime. If at the end of the day, a data protection analysis concludes that there is no risk to an individual's privacy, then the organisation is entitled to process the personal data.

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.

This analysis clarifies the interaction between the Data Protection Act and services such as Street View, or the vexed question of whether or not an IP address is personal data. We show that such information can be transformed, **unambiguously**, into personal data and provide the necessary proof. Data used for profiling individual users, if linked to that IP address and the individual can easily be transformed into personal data. Similarly, data linked to reference numbers in cookies can, unambiguously, become personal data.

In this analysis, we identify what a service provider should do in order to avoid data protection problems arising from this analysis; Appendix A lists the actions that are needed. We also provide advice to those individuals who do not want, for example, their browsing habits profiled for a marketing purposes; Appendix B contains a draft pro-forma e-mail based on this analysis.

Our analysis is illustrated by reference to the UK's Data Protection Act 1998. We show that it is very likely to apply to all individuals living in countries that have implemented the Data Protection Directive 95/46/EC[3] into national law, and to regimes that have data protection law based on the OECD Guidelines.[4]

[3] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data.*

[4] *The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980*

AN ANALYSIS BASED ON THE UK'S DATA PROTECTION ACT

To reach our conclusions, the analysis first has to focus on three questions:

1. Are data such as an IP address or a URL "personal data"?
2. If so, when can such personal data be legitimately processed?
3. Does the right to object to the processing of personal data apply?

Q1 Are data such as an IP address or a URL, "personal data"?

Any data protection regime, if it is to be engaged, needs personal data to be processed; in the definition of "personal data" in the UK's Data Protection Act, the relevant parts of the definition are emphasised below:

> " '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..." (our emphasis).

This leads to three considerations that will be familiar to those who attend our ISEB data protection courses.

1. **Is the information that is processed defined as "data"[5] under the Act?** The answer is "YES", because the information (e.g. street image, IP address) is processed automatically.

2. **Do the "data" relate to living individual who can be identified from the data or other information in the possession of the "data controller"[6]?** Many service providers know that the data retained during a session relate to an **identified** individual subscriber of internet services. For instance, authentification of an individual subscriber prior to permitting access to the service, or if access to a service is linked to billing arrangements, often imply there is the necessary identifying information in a service provider's possession. In some cases, this identifying information remains in

[5] *Data includes any automatically processed information. With internet applications, therefore, we have not considered the links to information held in manual form.*

[6] *The "data controller" is the organisation that determines the purpose of the processing and the manner in which personal data are processed*

possession of the service provider because it has to be retained for law enforcement purpose.

3. **Is it "likely" that the "other information" which leads to an individual being identified will "come into the possession of the data controller"**? This question only arises when a service provider does not possess the "other information" that can lead to identification of an individual.

It is important to note that the relevant test posed is: "whether the other identifying information is in the possession of, or likely to come into its possession of, the data controller". This test of "possession" **does not** depend on the data controller's use of the other identifying information in his possession; mere possession of both the "data" and "the other information" (or the likelihood of possession of "the other information") suffices to ensure that the "data" are treated as "personal data".

Although we have used the UK's Data Protection Act to illustrate the issue of identifiability, it is important to note that Directive 95/46/EC arrives at the same conclusion through its use of "an identified **or** identifiable natural person" in its definition of "personal data" in Article 2. The separate use of "identified individual **or** identifiable natural person" means that the definition relates to any individual who is currently identified **and** to any individual who is not currently identified but likely to be identified in future (e.g. identified by other information likely to come into the possession of the data controller).

Likewise with the OECD Guidelines[7]; it defines personal data to be "any information relating to an identified **or** identifiable individual (data subject)". Finally we note that Google's own privacy policy permits this option. It defines "personal information" to be "information that you provide to us which personally identifies you, such as your name, email address or billing information, **or other data which can be reasonably linked to such information by Google**"[8] (our

[7] *The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980*

[8] *http://www.google.com/privacy_glossary.html#personalinfo (text as of March 11, 2009)*

emphasis throughout). In other words, the mechanism suggested in this article could have global application to any data protection regime.

Ensuring the "other information" is in the data controller's possession

Google's processing of Street View images involves the use of technology that blurs faces and car number-plates. This from Google's perspective helps anonymise the individuals. However, in relation to individuals, identification is not from the face alone. A number of traits – for example, clothes, gait, height, weight and location – captured on camera often means that neighbours and friends can identify the individual concerned. Indeed, it is often neighbours and friends who point out to an individual that his or her outline is being displayed on Street View.

So, if such an individual were to complain to Google in the form "The outline of the individual photographed outside 55 Zebra Terrace on photograph (URL or reference number) is myself, Ms. Freda Bloggs who lives at 36 Acacia Avenue, London N7 6YH", then Google will gain "other information" into its possession that identifies the individual concerned. In such cases, the Street View data is now linked to identifying information that relates to a particular individual **who is now identified**. It follows that images of the blurred individuals are unambiguously personal data and that the individual concerned is the "data subject" in relation to those personal data. The Data Protection Act is then certainly engaged in relation to any **further** processing of these personal data.

Similarly with images of a detached house that an individual owns? If an owner says something like "the picture of 55 Acacia Avenue, London N7 6YH on photograph URL-reference is the home of Ms Freda Bloggs", then the Street View data plus the other information now in Google's possession would become comparable to that held on in many marketing lists. The identifying information provided by the house owner in a complaint has transformed the picture of the house data into personal data of the data subject. (In the UK, the type of house - detached houses are desirable and expensive - or where a specific individual lives can give an indication of the individual's wealth or socio-economic grouping. This

could be linked to Land Registry details that can be publicly available - county court judgment, debt recovery and bankruptcy proceedings).

Similarly, also with temporary IP address[9] associated with an individual user during an internet session. For example, suppose the user informs a service provider that "IP address 84.134.195.144 on 5th January, from 10.00am-11.00pm was used by Freda Bloggs of 55 Acacia Avenue, London N7 6YH", then this information would transform data linked to these IP details into personal data about Freda Bloggs.

The frequency of such complaints will be an important consideration. As more and more individuals contact a service provider in order to disclose identifying details as described above, the more a service provider should anticipate that identifying details will come into his possession, and the more and more the argument will be that such identifying data details are "likely" to be received. This is because the frequency of contact from individuals has changed from one of "possibility" to one that is "likely". In which case, there will come a time when the number of contacts and frequency of contact is such that a service provider will be obliged to treat the data as personal data on **ALL** users (i.e. without the need for any further contacts from individuals).

This depends on whether contact from a user is "likely" rather than a "possibility"? For example, suppose there is a database of 1,000,000 IP addresses and one user contact. We would argue that contact from a specific individual is "possible" rather than "likely"? However, suppose there were 100,000 complaints – we would say that contact from any specific individual is "likely" rather than "possible"? In general, a statistical analysis surrounding the number of contacts, the frequency of contact, will depend whether the **all** the data should be treated as personal data. This in turn depends on how individuals view a particular service; the more the suspicion about a service, the more there will be contacts from users. Indeed, given

[9] *A user's IP addresses can be obtained from www.myipaddress.com or www.myipnumber.com etc*

the nature of the Internet, we expect the emergence of software applications from consumer and privacy advocates that users can freely download that will set up the necessary contact.

Note that this mechanism still provides "personal data" even if a service provider uses an IP address in real time (e.g. a service provider that monitors IP addresses to deliver marketing messages and where all IP details are deleted as soon as the user's internet session is ended). All the user has to do is send a complaint e-mail (containing IP address, name, address) to the service provider's authorised or official contact point at the start of the internet session. It follows that the service provider is processing personal data for the duration of the session (and fair processing obligations will apply – see later).

Application to the use of cookies

A cookie "is a piece of information in the form of a very small text file that is placed on an internet user's hard drive. It is generated by a web page server, which is basically the computer that operates a web site. The information the cookie contains is set by the server and it can be used by that server whenever the user visits the site. A cookie can be thought of as an internet user's identification card, which tell a web site when the user has returned" Cookies are subject to regulation[10] and require the user to be "provided with clear and comprehensive information about the purposes of the storage of, or access to, that information" and "is given the opportunity to refuse the storage of or access to that information"[11].

Many cookies are associated with a reference number (and occasionally name linked personal data but not always). Since cookies reside on the user's computer they can be accessed by software applications. Once accessed, any reference number can be linked to the name and email address of the user, and this information (linked to the cookie information, times and IP address) can be

[10] *Regulation 6 of the Privacy and Electronic Communications (EC Directive) Regulations 2003*

transmitted to a service provider (and links to any profile held by the web-page server). In other words, the provision of identifying information by the user have the potential transform the cookies (and what they link to) unambiguously into personal data

All this of course is for the future. However, it is reasonable to anticipate that consumer and pro-privacy groups would develop software applications to automate such e-mail complaints to service providers if they thought this necessary. This is especially the case outside Europe (where the Privacy in the Electronic Communications Directive does not apply).

The argument is supported by Recital 26 of Directive 95/46/EC

Recital 26 supports the notion that it is legitimate for an individual to provide the identifying details to a data controller. This Recital states that:

> "Whereas the principles of protection must apply to any information concerning an identified **or** identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller **or by any other person to identify the said person**; whereas the' principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable";(our emphasis)

The emphasised words clearly include the possibility that identification of an individual is possible "by any other person" (i.e. other than the data controller). What can be more natural than the data subject contacting the data controller to identify that certain data relates to him with the consequence that such data should be treated as personal data **in any further processing?**

Note that a service provider cannot argue that he has no plans to use this other identifying information that has been sent to him as part of a complaint. As we have already remarked, the test posed by the definition of personal data is

---

[11] *Quotes from* http://www.aboutcookies.org *for information about cookies*

"whether the other identifying information is in its possession or likely to come into its possession" – not that such identifying information is actually used. Indeed, if a service is controversial, then the prudent service provider should anticipate that the other identifying information will be received.

However, in handling a complaint, as will be seen, it may be legitimate for the service provider to take reasonable steps to satisfy himself as to the identity of the complainant and the nature of the complaint. Identification of the data subject is obligatory if a complainant wants to exercise the right of access to personal data.

Q2. When can "personal data" be legitimately processed?

Google's current policy in the UK is to remove images from Street View on request, and likewise Phorm state that it seeks consent for its processing (facilitated via a cookie) where consent can be freely withdrawn. So in practice in the UK, if there is a complaint, there is no further processing in relation to these services. However, what would happen if another service provider (in UK terms, a "data controller") did not adopt this policy?

Assume an individual has made a complaint so that the service provider is in possession of the identifying information. In data protection terms, any **further** processing[12] of personal data (i.e. that processing from **after** the time of receipt of the complaint) has to be legitimised in terms of criteria set out in Schedule 2 of the Data Protection Act (or in Article 7 of Directive 95/46/EC).

These criteria provide for a number of justifications as to why, for example, IP personal data could continue to be processed by internet service providers. Different criteria justify a range of activities; for example:

[12] *"Processing" is a defined to mean any operation performed on the personal data – for instance, use, collect, retain, disclose or access*

(a) the "data subject could have unambiguously given his consent" to an activity. In the context of this analysis where the data subject has made a complaint, further processing relying on data subject consent cannot make any sense. In any event, consent is defined in the Directive as "freely given", "fully informed" where the data subject has signified agreement; by complaining, the data subject is signifying disagreement.

(b) The processing of personal data is associated with an activity 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 a contract". This could apply to any service which requires the processing of an IP address (e.g. in order to send information via the internet to a subscriber, a service provider must process the subscriber's IP address). The word "necessary" is an important limitation on the purpose of the processing; it stops a data controller specifying, in a contract, those purposes that are merely "useful" or "convenient".

(c) The processing of personal data could be associated with an activity that is "necessary for compliance with a legal obligation to which the data controller is subject". This arises when law enforcement agencies require private bodies to retain of records of internet use or searches; for instance, European countries often enact laws that require data retention in accordance with Directive 2006/24/EC[13].

(d) The processing is necessary in order to protect the vital interests of the data subject – for example, in life or death situations.

(e) The processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller, usually in connection with a public service delivered by a statutory public body such as a police

[13] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*

force, government department, NHS Trust or local authority. This provision obviously covers the processing of IP addresses by the authorities in relation to say terrorism, crime, law enforcement, public emergences etc; or

(f) The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests of the data subject. This is discussed in the next section as it is usually the criterion where the data subject has most leverage.

The rest of the analysis assumes that it is this last paragraph (f) that would form the legal basis for any further processing of personal data. This would be the case with "Street View" if Google did not take details down on request.

Suppose personal data were to be further processed?

If personal data (e.g. data linked to identifying detail provided by the individual concerned) were to be further processed, and none of the other five criteria (a) to (e) specified above are relevant then under the UK's Data Protection Act any continued processing could be justified in terms of criteria (f) above. In further detail, this criteria (paragraph 6 of Schedule 2) reads as follows:

6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

In practice, the paragraph requires the data controller (in this case, the service provider) to balance his own legitimate interests served by the processing (or the legitimate interests of a third party user of the personal data) with the legitimate interests of the data subject (in this case, the individual user of the service) in the processing not occurring. This balance starts in favour of the data controller except in those circumstances where the prevailing legitimate interests of the data subject can be identified. However, if a data subject has submitted a complaint (providing

the identifying information and reasons for the complaint), the data subject has warned the data controller of his opinion that his legitimate interests should prevail.

The data subject's legitimate interest might be a security concern or any other credible reason why the processing of personal data should be stopped. Note that in this exchange, it is perfectly reasonable for the data controller to ask the data subject why his legitimate interests should prevail, or to identify why the data controller's legitimate interest in continued processing should prevail.

Additionally, any further processing of personal data by the service provider has to comply with obligations found in other data protection principles (e.g. security, retention, relevance, fairness). For example, if a data controller decides to continue the processing of personal data **after** a complaint, he is likely to need to issue a Fair Processing Notice to identify the data controller and the purposes of the processing and anything else necessary to guarantee fair processing. A contact address provided by the data subject in the complaint can help ensure that such a notice can be given. In this case, it has been assumed that a Fair Processing Notice has not been issued because the service provider had not hitherto recognised that he was processing personal data.

Finally, if the use of personal data was for a marketing purpose, the complaint in terms of the processing of personal data for a marketing purpose should always prevail in favour of the data subject as there is an absolute right to object to a marketing purpose[14].

Q3 Does the right to object to the processing of personal data apply?

Suppose Google changed its policy with respect to Street View and decided that it was in its legitimate interest to continue the processing of personal data despite a

[14] *Section 11 of the Data Protection Act or Article 14b of Directive 95/46/EC*

complaint from a data subject. If this were to happen the right to object[15] to the processing would become very useful weapon in the armoury of the data subject.

This right to object buttresses the position of a data subject where the data controller is processing personal data and has assessed the balance of legitimate interests in favour of the data controller and continues to process the personal data despite a complaint from a data subject. Appendix B provides a template for such a complaint and exercising the right to object. As indicated previously, this right to object does not apply in the case of an objection to the processing of personal data for a marketing purpose because there is a separate right relating to that marketing purpose that **must** prevail in the data subject's favour.

The right to object to the processing of personal data under UK law (which also exists in all European Data Protection laws based on the Directive) states that if a data subject can show that the processing of the personal data or "is causing or is likely to cause substantial damage or substantial distress to him or to another, and that damage or distress is or would be unwarranted" then the processing must cease. Note the threshold also requires the data subject to raise an issue of substance and to show the unwarranted nature of the processing (e.g. security threat).

On receipt of a request for cessation of the future processing, the data controller "must within twenty-one days of receiving a notice ... give the individual who gave it a written notice (a) stating that he has complied or intends to comply with the data subject notice, or (b) stating his reasons for regarding the data subject notice as to any extent unjustified and the extent (if any) to which he has complied or intends to comply with it". Similarly, with respect to the right of access, the data controller has to respond to the data subject.

If this written notice does not arrive or the processing continues despite objection, the data subject then can ask the Information Commissioner to assess whether or

[15] *Section 10 of the Data Protection Act 1998*

not the data controller is respecting the rights of data subjects. This allows for an independent assessment of the facts of a particular objection; the data controller is likely to have to justify his decision not to halt the processing. Note that it does **not** mean that the processing has to cease because of an objection from a data subject. With any assessment by an independent body, the assessment can easily be in favour of the service provider.

Does the right of access to personal data apply?

Note that individuals can provide identifying information in order to engage the right of access to personal data held by a service provider. For instance, if an individual says "I wish to have a copy of personal data related to the use of IP address 84.134.195.144 on 5th January, from 10.00am-11.00pm" and provides the relevant identification details (e.g. Freda Bloggs of 55 Acacia Avenue, London N7 6YH), then individuals should receive all such personal data (assuming there are no applicable exemptions and the personal data are still held and the service provider is satisfied as to the applicant's identity).

However, following Durant[16], the right of access does not provide access to every data item that can be associated with a data subject's personal data. The right only extends to those personal data that directly relates to the applicant such as websites visited, or search terms entered by that individual. The right does not give access to technical data that are more associated with supporting a user session (e.g. what disks were used to store personal data or information prior to it transmitted to an individual's computer). This argument might extend to arguments that a picture of a property was not personal data, if the property was a high-rise block of flats as the data could relate to many individuals rather than a specific individual.

---

[16] The Durant decision in the Court of Appeal (Neutral Citation No: [2003] EWCA Civ 1746) limited personal data to that information that relates to the individual directly. For example, if a name is entered into Google's search engine, not all the returned links relate to that individual – some of them will, some of them won't.

WHAT ARE THE COUNTER ARGUMENTS?

There are three possible counter arguments. First a service provider might argue that the provision of "other identifying information" by the data subject is an artificial device designed to engage the Act. Surely, the argument goes, the law does not require an organisation to be subject to the onerous obligations of a data controller merely at the whim of an individual? So, for example, a data controller might decide to delete the identifying information that has been sent by the data subject in order to get back to the status quo prior to a complaint.

However, the interpretation of Recital 26 as identified earlier (which allows for the data subject to identify himself to the data controller) should mitigate against this strategy. If Recital 26 suggests that the data controller should take account "of all the means likely reasonably to be used ... **by ...any other person**" to identify the data subject, deletion of the identifying data by the service provider serves the opposite objective; namely to take **no** account of a very simple identification mechanism and thereby evade all data protection obligations of the data controller.

Deletion of the identifying information would have to be justified in terms of an attempt to render the personal data anonymous; it is likely to encounter difficulties with the part of Recital 26 which states that "whereas the' principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable".

The fact that only three or four items of identifying information are needed (e.g. name, IP address, time of use of service) to transform the data into personal data, shows that the data with name linked data removed possess a very minimal degree of anonyminity. If the data were truly anonymous, then provision of a name and IP address etc. would not have any effect on the degree of anonymisation of the data.

Evidence for this view can be derived from the case CSA v SIC[17], where the House of Lords considered the application of Recital 26 in the context of statistical

[17] *Judgments - Common Services Agency (Appellants) v Scottish Information Commissioner (Respondent) (Scotland) SESSION 2007-08, [2008] UKHL 47*

information, derived from sensitive personal data, that had been minimally anonymised through a technique known as barnardisation. Paragraph 26 of this judgement states that the degree of anonymisation should be a very high one (i.e. one of near impossibility), and by implication that a minimal degree of anonymisation is not one described by Recital 26.

> "...The question is whether the data controller, or anybody else who was in possession of the barnardised data, would be able to identify the living individual or individuals to whom the data in that form related. If it was **impossible** for the recipient of the barnardised data to identify those individuals, the information would not constitute "personal data" in his hands (our emphasis of paragraph 26).

The second argument can be summarised as the "found pay as you go mobile phone" scenario. Suppose someone finds a pay as you go mobile, switches it on provides the telecommunications company with his name, address SIM card number and phone number, and asks the telecommunications company: "Now provide details of the numbers called from this phone". How do you know that the person who asks for the details is the owner of the phone? In our case, how do you know the user of a computer is the user who did the browsing, if more than one user can use the computer?

On analysis, this argument depends not on whether the data are personal data, but rather of the authenticity of the individual's claim to be the data subject. In such cases, other information might be needed to authenticate the data subject's claim. As indicated in the text previously, it is reasonable for the data controller to be satisfied as to the identity of a complainant when considering the exercise of data subject rights (e.g. right of access or to object to the processing). This could take the form of information known to the data subject and held by the service provider (e.g. the date and time of the log-in to and log-off from the internet access service[18] or which web-sites were visited (if these are retained by the service provider). Finally, it should be noted that an individual who impersonates a data

[18] *The Data Retention Directive (see reference 16) requires this data to be held*

subject can commit an offence[19] and this prospect acts as a deterrence. In summary, we do not see the "lost pay as you go mobile" scenario as undermining the argument presented here.

The third argument involves a decision of the High Court in the case of Ezsias[20]. In this case, there was a subject access request following an employment dismissal; the claimant wrote extensively to the National Assembly for Wales to complain about the actions of a NHS Trust. This correspondence generated about 2,500 pages of documents, and included several lengthy subject access requests to the personal data in those documents. The judgment suggested, controversially, that a data controller is only obliged to carry out "reasonable and proportionate" steps to identify and disclose personal data.

The argument might be raised that it is "reasonable and proportionate" to disregard the data subject's communications that provide the identifying information, as its purpose is to unreasonably or disproportionately engage the Act.

However, we are of the view that there are several distinguishing features that negate the claim that Ezsias provides a precedent. For example:

- In Ezsias, the data subject provided hundreds of pages of documents containing personal data; by contrast, the provision of information by the data subject is limited to a few items (e.g. name and IP address).

- In Ezsias, most of the personal data referred to by the Court were provided by the data subject; this contrasts with a situation where most of the personal data are processed by the service provider and where the personal data contains information that can possess considerable biographical significance for the data subject (e.g. websites visited, downloads, personal lifestyle choices etc).

---

[19] *S.55 of the Data Protection Act 1998*

[20] *Ezsias v Welsh Ministers ([2007] All ER (D) 65 (Dec))*

- In Ezsias, the personal data were in unstructured manual form; this contrasts with the internet data where personal data are automatically processed and easily searchable by computer.

- In Ezsias, the case revolved around the right of access to personal data already held by a data controller; this contrasts with a focus on the exercise of the right to object to **future** processing of personal data by the controller.

CONCLUDING COMMENTS

We believe that the above arguments are persuasive enough to show that data containing IP data, cookie related data or a Street View URL etc should be treated as personal data if individuals, if at any time, can provide the necessary identifying details in a complaint.

The more controversial the service, the more complaints will be generated, the more data will be transformed into personal data. That is why a prudent service provider could conclude that, depending on the nature of the service, they need consider treat data as if they were personal data at the outset and without the need for any individual to send a complaint.

Indeed, there is now a simple test of whether or not certain information linked to an IP address, reference number or URL is personal data. If the individual concerned provides the necessary identifying information, then the data ARE personal data. If sufficient individual users each provide the necessary identifying details, then the data linked to ANY individual should be considered to be personal data.

In summary, the fact that data linked to a URL or IP address can become personal data at any time empowers users to control their own privacy on the Internet.

Dr. C. N. M. Pounder,
Amberhawk Training Ltd,
July 2009
info@amberhawk.com

APPENDIX A: ACTION POINTS FOR SERVICE PROVIDERS

1. Make sure your privacy officer/data protection officer understands the nuances of the legal basis for the argument presented here; if not get him trained. It is not enough to understand the outline of the argument as all the other subsequent data protection consequences of the fact that personal data are processed can apply to the service (e.g. data retention policies)

2. Decide whether the complaints mechanism described here applies to your services; remember sometimes it won't (e.g. if your processing of personal data is necessary for a contract or a statutory obligation)

3. If data subjects can use this mechanism, review procedures related to your processing of internet data (e.g. IP address) so they can accommodate complaints from data subject. Provide an prominent access point so that data subjects can make their objections in a controlled way; this makes the easier to manage. (Have a look at Appendix B – this is how we would complain).

4. Decide whether you will want any complaint to be subject to the applicant providing identification or reasonable cause. If you require this and you refuse the applicant, anticipate the subsequent use of the right of access to personal data or the right to object to the processing or a request for an assessment from the Information Commissioner.

5. Check your privacy policy and modify any fair processing notice to describe your processing of personal data that subsequently arises; include a description of the complaints mechanism in the notice.

6. Make sure that subject access procedures can retrieve personal data when provided with a IP address or URL or what the data subject provides.

7. Keep data subjects informed and keep records as to any complaint.

8. Keep to any relevant time limits specified in data protection legislation that need to be considered (e.g. 40 days for subject access).

9. APPENDIX B: DRAFT E-MAIL/LETTER FOR DATA SUBJECTS.

(Send recorded receipt, delivery or read to an official/authorised access point**)**

36 Acacia Avenue,
London N7 6YH
Date:
Email: xxx@yyy.com

IMPORTANT: this provides the identifying link to the personal data
Fix the time of the e-mail/letter
For ease of contact

Objection to the processing of personal data

Dear Service Provider

Can I identify myself (Freda Bloggs) as being the individual photographed on Street View at ..... Your reference for the photograph(s) is/are ..... and my full contact details are given above

or

Can I identify myself (Freda Bloggs) as using IP address ..... on **date/time** .....; my contact details are given above.

As you are now processing photograph/IP personal data linked to an identified individual, I would ask you to cease processing of my personal data within a reasonable timescale. The reason why I would like the processing to cease is .....; ***something credible and particular to the data subject***)

{If you to decide to continue your processing of my personal data the law requires you to issue a fair processing notice; I cannot recall receiving such a notice. For convenience you can use the e-mail I have provided} (***Optional and only if relevant***)

If you processed my personal data on the basis of my consent, can you take this note to mean that consent has now been withdrawn; any processing of my personal data for a marketing purpose should also cease within a reasonable time.

I understand that you can continue any processing of my personal data if it is necessary for my contract or pursuant to a statutory obligation or statutory function. If these conditions do not apply, and you continue to process my personal data, please consider this note as my formal application of the right to object to your continued processing of my personal data.

Yours sincerely,

Freda Bloggs

APPENDIX C: ADVERTS

DATA PROTECTION FOR USA AND EUROPEAN PRIVACY OFFICERS

We have developed a course to provide USA and European privacy officers with rounded knowledge of European Data Protection law based on the Directive 95/46/EC and the Privacy & Electronic Communications Directive 2002/58/EC (the latter in the context of e-commerce). An assessment of understanding can be obtained by written exam – this is a variant of the data protection qualification for the UK offered by the ISEB, a qualification body linked to the British Computer Society. The ISEB have told us they are prepared to set an exam. If interested please contact ***info@amberhawk.com***.

COURSES FOR DATA PROTECTION OFFICERS IN THE UK

Amberhawk provides a wide range of public training suitable for data protection officers in the UK. These include courses leading to the ISEB qualification in data protection. With respect to on-site training, Amberhawk can provide sector specific training (e.g. on rights of access, PECR, CCTV, Human Resources, Data sharing) as well as on-site ISEB courses.

We have a Data Protection Audit courses as well as a course on Level 1 of the Government's Information Assurance Strategy (the HMG Security Framework). If interested please contact us at ***info@amberhawk.com***

COURSES IN FREEDOM OF INFORMATION

Amberhawk provides a wide range of public training suitable for those dealing with Freedom of Information and the Environmental Information Regulations. These include courses leading to the ISEB qualification. With respect to on-site training, Amberhawk can provide sector specific training aimed at those helping a public authority meet its obligations. Courses can include Re-use Regulations by Public Sector Bodies.

If interested please contact us at ***info@amberhawk.com***